NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

CIS

Congressional Information Service, Inc.
Washington, D.C.

Office of Technology Assessment

Congressional Board of the 99th Congress

TED STEVENS, *Alaska, Chairman*

MORRIS K. UDALL, *Arizona, Vice Chairman*

Senate	House
ORRIN G. HATCH *Utah*	GEORGE E. BROWN, JR. *California*
CHARLES McC. MATHIAS, JR. *Maryland*	JOHN D. DINGELL *Michigan*
EDWARD M. KENNEDY *Massachusetts*	CLARENCE E. MILLER *Ohio*
ERNEST F. HOLLINGS *South Carolina*	COOPER EVANS *Iowa*
CLAIBORNE PELL *Rhode Island*	DON SUNDQUIST *Tennessee*

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

WILLIAM J. PERRY, *Chairman*
H&Q Technology Partners

DAVID S. POTTER, *Vice Chairman*
General Motors Corp. (Ret.)

EARL BEISTLINE
Consultant

CHARLES A. BOWSHER
General Accounting Office

CLAIRE T. DEDRICK
California Land Commission

JAMES C. FLETCHER
University of Pittsburgh

S. DAVID FREEMAN
Lower Colorado River Authority

JOSEPH E. ROSS
Congressional Research Service

MICHEL T. HALBOUTY
Michel T. Halbouty Energy Co.

CARL N. HODGES
University of Arizona

RACHEL McCULLOCH
University of Wisconsin

LEWIS THOMAS
Memorial Sloan-Kettering Cancer Center

Director

JOHN H. GIBBONS

The Technology Assessment Board approves the release of this report. The views expressed in this report are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

Federal Government Information Technology

Electronic Record Systems and Individual Privacy

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D. C. 20510

J 952-53

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

Library of Congress Catalog Card Number 86-600524

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC 20402

Foreword

Public policy on the protection of personal information collected, maintained, or disseminated by the Federal Government has been based on a balancing of the privacy of individual citizens versus management efficiency and law enforcement. New technological applications—such as the computerized matching of two or more sets of records, extensive electronic networking of diverse computerized record systems, and preparation of computer-based profiles on specific types of individuals—are challenging the existing statutory framework for balancing these interests.

This report addresses four major areas: 1) technological developments relevant to government record systems; 2) current and prospective Federal agency use of electronic record systems; 3) the interaction of technology and public law relevant to protecting privacy; and 4) possible policy actions that warrant congressional attention, including amendment of existing laws such as the Privacy Act of 1974 and establishment of new mechanisms such as a Data Protection Board or Privacy Protection Commission.

Prepared at the request of the Senate Committee on Governmental Affairs and the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, this report is the third component of the OTA assessment of "Federal Government Information Technology: Congressional Oversight and Civil Liberties." The first component, *Electronic Surveillance and Civil Liberties*, was published in October 1985, and the second, *Management, Security, and Congressional Oversight*, was published in February 1986.

In preparing this report on electronic record systems and privacy, OTA has drawn on working papers developed by OTA staff and contractors, the comments of participants at an OTA workshop on this topic, and the results of an OTA survey that was completed by over 140 agency components. Drafts of this report were reviewed by the OTA project advisory panel, officials from the U.S. Office of Management and Budget and the General Services Administration; U.S. Departments of Justice, State, Defense, and Health and Human Services, among other Federal agencies; and a broad spectrum of interested individuals from the governmental, academic, private industry, and civil liberty communities.

OTA appreciates the participation of the advisory panelists, workshop participants, external reviewers, Federal agency officials, and others who helped bring this report to fruition. The report itself, however, is solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.

John H. Gibbons

JOHN H. GIBBONS
Director

Electronic Record Systems and Individual Privacy Advisory Panel

Theodore J. Lowi, *Chairman*
Professor of Political Science, Cornell University

Arthur G. Anderson
IBM Corp. (Ret.)

Jerry J. Berman
Legislative Counsel
American Civil Liberties Union

R.H. Bogumil
Past President
IEEE Society on Social Implications of Technology

James W. Carey
Dean, College of Communications
University of Illinois

Melvin Day
Vice President
Research Publications

Joseph W. Duncan
Corporate Economist
The Dun & Bradstreet Corp.

William H. Dutton
Associate Professor of Communications and Public Administration
Annenberg School of Communications
University of Southern California

David H. Flaherty
Professor of History and Law
University of Western Ontario

Carl Hammer
Sperry Corp. (Ret.)

Starr Roxanne Hiltz
Professor of Sociology
Upsala College

John C. Lautsch
Chairman, Computer Law Division
American Bar Association

Edward F. Madigan
Office of State Finance
State of Oklahoma

Marilyn Gell Mason
Director
Atlanta Public Library

Joe Skinner
Corporate Vice President
Electronic Data Systems Corp.

Terril J. Steichen
President
New Perspectives Group, Ltd.

George B. Trubow
Director, Center for Information Technology and Privacy Law
The John Marshall Law School

Susan Welch
Professor and Chairperson
Department of Political Science
University of Nebraska

Alan F. Westin
Professor of Public Law and Government
Columbia University

Langdon Winner
Associate Professor of Political Science
Rensselaer Polytechnic Institute

Congressional Agency Participants

Robert L. Chartrand
Senior Specialist
Congressional Research Service

Robert D. Harris
Deputy Assistant Director for Budget Analysis
Congressional Budget Office

Kenneth W. Hunter
Senior Associate Director for Program Information
U.S. General Accounting Office

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the advisory panel members. The panel does not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

OTA Electronic Record Systems and Individual Privacy Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Fred W. Weingarten, *Manager*
Communication and Information Technologies Program

Project Staff

Fred B. Wood, *Project Director*
Jean E. Smith, *Assistant Project Director*
Priscilla M. Regan, *Principal Author and Analyst*
Jim Dray, *Research Analyst*
Jennifer Nelson, *Research Assistant*

Administrative Staff

Elizabeth A. Emanuel, *Administrative Assistant*
Shirley Gayheart,* *Secretary*
Audrey Newman, *Secretary*
Renee Lloyd, *Secretary*
Patricia Keville, *Clerical Assistant*

Contractors

William Dutton and Robert Meadow
The University of Southern California

David H. Flaherty
The University of Western Ontario

Karen B. Levitan, Patricia D. Barth, and Diane Griffin Shook
The KBL Group, Inc.

Robert Ellis Smith
The Privacy Journal

---

*Deceased, Dec. 11, 1985.

OTA Electronic Record Systems and Individual Privacy Workshop

Robert Belair
Attorney
Kirkpatrick & Lockhart

William Cavaney
Executive Secretary
Defense Privacy Board
U.S. Department of Defense

Louis D. Enoff
Acting Deputy Commissioner for Programs
and Policy
Social Security Administration

Robert Freeman
Committee on Open Government
Department of State
State of New York

John Gish
Vice President
W.R. Grace & Co.

John Grace
Privacy Commissioner of Canada

Richard P. Kusserow
Inspector General
U.S. Department of Health and
Human Services

Robert Meadow
Professor, Annenberg School of
Communications
University of Southern California

Philip Natcharin
Director of Program Integrity
New York State Department of
Social Services

Robert Oakley
Assistant Inspector General for Auditing
Veterans Administration

Alan Rodgers
Massachusetts Law Reform Commission

James Rule
Professor, Department of Sociology
State University of New York at
Stony Brook

Andy Savitz
Assistant Secretary of Administration
and Finance
State of Massachusetts

Robert Ellis Smith
Editor
The Privacy Journal

Jane Tebbutt
Office of Inspector General
U.S. Department of Health and
Human Services

Tom Tiffany
Acting Director of Legislative Affairs
Internal Revenue Service

Rob Veeder
Desk Officer
Office of Information and
Regulatory Affairs
Office of Management and Budget

Contents

Chapter *Page*

1. Summary 3

2. Electronic Record Systems and the Privacy Act: An Introduction 11

3. Computer Matching to Detect Fraud, Waste, and Abuse 37

4. Computer-Assisted Front-End Verification 67

5. Computer Profiling 87

6. Policy Implications 99

Appendix

A. Update on Computerized Criminal History Record Systems 129

B. OTA Federal Agency Data Request 135

C. List of Contractor Reports 145

D. Other Reviewers and Contributors 146

E. Summary of Final Rules for Income and Eligibility Verification Required Under the Deficit Reduction Act of 1984 147

F. Privacy and Data Protection Policy in Selected Foreign Countries 150

Chapter 1

Summary

Chapter 1

Summary

INTRODUCTION

All governments collect and use personal information in order to govern. Democratic governments moderate this need with the requirements to be open to the people and accountable to the legislature, as well as to protect the privacy of individuals. Advances in information technology have greatly facilitated the collection and uses of personal information by the Federal Government, but also have made it more difficult to oversee agency practices and to protect the rights of individuals.

In 1974, Congress passed the Privacy Act to address the tension between the individual's interest in personal information and the Federal Government's collection and use of that information. The Privacy Act codified principles of fair information use that specified requirements agencies were to meet in handling personal information, as well as rights for individuals who were the subjects of that information. To ensure agency compliance with these principles, the act enabled individuals to bring civil and criminal suits if information was willfully and intentionally handled in violation of the act. In addition, the Office of Management and Budget (OMB) was assigned responsibility for overseeing agency implementation of the act.

At the time the Privacy Act was debated and enacted, there were technological limitations on the use of individual records by Federal agencies. The vast majority of record systems in Federal agencies were manual. Computers were used only to store and retrieve, not to manipulate or exchange information. It was theoretically possible to match personal information from different files, to manually verify information provided on government application forms, and to prepare a profile of a subset of individuals of interest to an agency. However, the number of records involved made such applications impractical.

In the 12 years since the Privacy Act was passed, at least two generations of information technology have become available to Federal agencies. Advances in computer and data communication technology enable agencies to collect, use, store, exchange, and manipulate individual records in electronic form. Microcomputers are now widely used in the Federal Government, vastly increasing the potential points of access to personal record systems and the creation of new systems. Computer matching and computer-assisted front-end verification are becoming routine for many Federal benefit programs, and use of computer profiling for Federal investigations is expanding. These technological advances enable agencies to manipulate and exchange entire record systems, as well as individual records, in a way not envisioned in 1974. Moreover, the widespread use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a *de facto* national database[1] containing personal information on most Americans. And use of the social security number as a *de facto* electronic national identifier facilitates the development of this database.

These technological advances have opened up many new possibilities for improving the efficiency of government recordkeeping; the detection and prevention of fraud, waste, and abuse; and law enforcement investigations. At the same time, the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. Because of the expanded access to and use of personal information in decisions about individuals, the completeness, accuracy, and relevance of information is even more important. Additionally, the expanded access and use make it nearly impossible for individuals to learn about, let alone seek redress for, misuse of their records. Even within agencies, it is often not known what applications of personal information are being used. Nor do OMB or relevant congressional committees know whether personal information is being used in conformity with the Privacy Act.

---

[1] The term *de facto* national database is used to distinguish it from a national database that was created by law, i.e., a *de jure* national database.

Overall, OTA has concluded that Federal use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many of the electronic record applications being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered by the act or by subsequent OMB guidelines. The rights and remedies available to the individual, as well as agency responsibilities for handling personal information, are not clear. Even where applications are covered by the Privacy Act or related OMB guidelines, there is little oversight to ensure agency compliance. More importantly, neither Congress nor the executive branch is providing a forum in which the conflicts—between privacy interests and management or law enforcement interests--generated by Federal use of new applications of information technology can be debated and resolved. Absent such a forum, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

POLICY PROBLEMS

OTA's analysis of Federal agency use of electronic record systems, specifically for computer matching, front-end verification, and computer profiling, revealed a number of common policy problems.

First, **new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves.** As a general principle, the Privacy Act prohibits the use of information for a purpose other than that for which it was collected without the consent of the individual. New computer and telecommunication applications for processing personal information facilitate the use of information for secondary purposes, e.g., use of Federal employee personnel information to locate student loan defaulters, or use of Federal tax information to evaluate a Medicaid claim.

The expanded use and exchange of personal information have also made it more difficult for individuals to access and amend information about themselves, as provided for in the Privacy Act. In effect, the Privacy Act gave the individual a great deal of responsibility for ensuring that personal information was not misused or incorrect. Technological advances have increased the disparity between this responsibility and the ability of the individual to monitor Federal agency practices. For example, individuals may not be aware that information about them is being used in a computer match or computer profile, unless they monitor the *Federal Register* or questions about them arise as a result of the application. In computer-assisted front-end verification, individuals may be notified on an application form that information they provide will be verified from outside sources, but are unlikely to be told which sources will be contacted.

Additionally, new computer and telecommunication capabilities enable agencies to exchange and manipulate not only discrete records, but entire record systems. At the time the Privacy Act was debated, this capability did not exist. The individual rights and remedies of the act are based on the assumption that agencies were using discrete records. Exchanges and manipulations of entire record systems make it more difficult for an individual to be aware of uses of his or her record, as those uses are generally not of immediate interest to the individual.

Second, **there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with**

the Privacy Act and related OMB guidelines. Under the Privacy Act, Federal agencies are required to comply with certain standards and procedures in handling personal information—e.g., that the collection, maintenance, use, or dissemination of any record of identifiable personal information should be for a necessary and lawful purpose; that the information should be current, relevant, and accurate; and that adequate safeguards should be taken to prevent misuse of information.

OMB is assigned responsibility for oversight of agency implementation of the Privacy Act. Prior studies by the Privacy Protection Study Commission (1977), the U.S. General Accounting Office (1978), and the House Committee on Government Operations (1975 and 1983) have all found significant deficiencies in OMB's oversight of Privacy Act implementation. For example, under the Privacy Act, information collected for one purpose should not be used for another purpose without the permission of the individual; however, a major exemption to this requirement is if the information is for a "routine use"—one that is compatible with the purpose for which it was collected. Neither Congress nor OMB has offered guidance on what is an appropriate routine use; hence this has become a catchall exemption permitting a variety of exchanges of Federal agency information.

Looking more specifically, OTA found that OMB is not effectively monitoring such basic areas as: the quality of Privacy Act records; the protection of Privacy Act records in systems currently or potentially accessible by microcomputers; the cost-effectiveness of computer matching and other record applications; and the level of agency resources devoted to Privacy Act implementation. OTA also found that neither OMB nor any other agency or office in the Federal Government is currently collecting or maintaining this information on a regular basis. Given the almost total lack of information concerning the activities of Federal agencies with respect to personal information, OTA conducted its own one-time survey of major Federal agencies and found that:

- the quality (completeness and accuracy) of most Privacy Act record systems is unknown even to the agencies themselves; few (about 13 percent) of the record systems are audited for record quality, and the limited evidence available suggests that quality varies widely;
- even though the Federal inventory of microcomputers has increased from a few thousand in 1980 to over 100,000 in 1985, very few agencies (about 8 percent) have revised privacy guidelines with respect to microcomputers;
- few agencies reported doing cost-benefit analyses either before (3 out of 37) or after (4 out of 37) computer matches; authoritative, credible evidence of the cost-effectiveness of computer matching is still lacking; and
- in most Federal agencies, the number of staff assigned to Privacy Act implementation is limited; of 100 agency components responding to this question, 33 reported less than 1 person per agency assigned to privacy and 34 reported 1 person.

Additionally, OTA found that there is little or no governmentwide information on, or OMB oversight of: 1) the scope and magnitude of computer matching, front-end verification, and computer profiling activities; 2) the quality and appropriateness of the personal information that is being used in these applications; and 3) the results and cost-effectiveness of these applications.

Third, **neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved.** The efficiency of government programs and investigations is improved by more complete and accurate information about individuals. The societal interest in protecting individual privacy is benefited by standards and protections for the use of personal information. Public policy needs to recognize and address the tension between these two interests.

Since 1974, the primary policy attention with respect to Federal agency administration has shifted away from privacy-related concerns. Interests in management, efficiency, and budget have dominated the executive and legislative agenda in the late 1970s and early 1980s. Congress has authorized information exchanges among agencies in a number of laws, e.g., the Debt Collection Act of 1982 and the Deficit Reduction Act of 1984. In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

A number of executive bodies have been established to make recommendations for improving the management of the Federal Government, e.g., the President's Council on Integrity and Efficiency, the President's Council on Management Improvement, and the Grace Commission. All have endorsed the increased use of applications such as computer matching, front-end verification, and computer profiling in order to detect fraud, waste, and abuse in government programs. However, these bodies have given little explicit consideration to privacy interests. Some executive guidelines remind agencies to consider privacy interests in implementing new programs, but these are not followed up to ensure agency compliance.

In general, decisions to use applications such as computer matching, front-end verification, and computer profiling are being made by program officials as part of their effort to detect fraud, waste, and abuse. Given the emphasis being placed on Federal management and efficiency, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. As a result, ethical decisions about the appropriateness of using certain categories of personal information, such as financial, health, or lifestyle, are often made without the knowledge of or oversight by appropriate agency officials (e.g., Privacy Act officers or inspectors general), OMB, Congress, or the affected individuals.

Fourth, **within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered.** The complexity of Federal Government relations—within executive agencies, between the executive and legislature, between the Federal Government and State governments, and between the Federal Government and the private sector—is mirrored in interconnecting webs of information exchanges. This complexity and interconnectedness is reflected in myriad laws and regulations, most of which have been enacted in a piecemeal fashion without consideration of other information policies.

Some of these policies may be perceived as being somewhat inconsistent with others, e.g., the privacy of personal information and public access to government information. Some laws and regulations may only partially address a problem, e.g., Federal privacy legislation does not include policy for the private sector or for the flow of information across national borders. In other instances, issues that are inherently related and interdependent, such as privacy and security, are debated and legislated in separate forums with only passing attention to their relationship.

Additionally, the Federal Government's information systems, as well as its information policy, are dependent on technological and economic developments. Federal funding for research and development and Federal financial and market regulations will have significant implications for information technologies and markets. Yet, under the present policymaking system, there is no assurance that these implications will be considered. Likewise, the international information policy environment, as well as international technological and economic developments, affects domestic information policy; again, these factors are not systematically considered in the existing policy arenas.

POLICY ACTIONS

OTA identified a range of policy actions for congressional consideration:

1. Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion. This would lead to continued uncertainty regarding individual rights and remedies, as well as agency responsibilities. Additionally, lack of congressional action will, in effect, represent an endorsement of the creation of a *de facto* national database and an endorsement of the use of the social security number as a *de facto* national identifier.
2. Congress could consider a number of problem-specific actions. For example:
    - establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of personal information, and the rights of individuals;
    - implement more controls and protections for sensitive categories of personal information, such as medical and insurance;
    - establish controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government, and provide for appropriate enforcement mechanisms;
    - review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness;
    - review issues concerning use of the social security number as a *de facto* national identifier and, if necessary, restrict its use or legislate a new universal identification number; or
    - review policy with regard to access to the Internal Revenue Service's information by Federal and State agencies, and policy with regard to the Internal Revenue Service's access to databases maintained by Federal and State agencies, as well as the private sector. If necessary, legislate a policy that more clearly delineates the circumstances under which such accesses are permitted.
3. Congress could initiate a number of institutional adjustments, e.g., strengthen the oversight role of OMB, increase the Privacy Act staff in agencies, or improve congressional organization and procedures for consideration of information privacy issues. These institutional adjustments could be made individually or in concert. Additionally or separately, Congress could initiate a major institutional change, such as establishing a Data Protection or Privacy Board or Commission.
4. Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which information privacy is a part.

ABOUT THE REPORT

Chapters 2 through 6 of this report provide technical and policy analyses relevant to electronic record systems privacy, and to proposed legislation such as: the "Data Protection Act of 1985" that would establish a Data Protection Board as an independent agency of the executive branch; possible amendments to the Privacy Act and Paperwork Reduction Act; and management improvement legislation.

Appendix A to this report updates trends and issues relevant to the privacy of information in computerized criminal history record systems, the subject of a prior OTA study. Appendix B describes the methodology of and respondents to the OTA survey (known officially as the OTA Federal Agency Data Request). Appendix C lists the OTA contractor papers relevant to this report. Appendix D lists the outside reviewers and contributors. Appendix E summarizes the Deficit Reduction Act regulations on front-end verification. Appendix F describes the privacy and data protection policies in selected countries.

Other components of this OTA assessment include the October 1985 OTA report on *Electronic Surveillance and Civil Liberties* that discusses issues and options relevant to electronic communications privacy, and the February 1986 OTA report on *Management, Security, and Congressional Oversight* that discusses, among other things, management, technical, and legal issues and options relevant to protecting the security (and, hence, privacy) of computer systems.

Chapter 2

Electronic Record Systems and the Privacy Act: An Introduction

Contents

Page

Summary 11

Introduction 12

Background 13
  Privacy 13
  History of the Privacy Act 14
  Implementation of the Privacy Act 16
  Requirement 1 17
  Requirement 2 18
  Requirement 3 19
  Requirement 4 20
  Requirement 5 21
  Requirement 6 21

Findings 22
  Finding 1 22
  Finding 2 25
  Finding 3 26
  Finding 4 29

Tables

Table No. *Page*

1. Statutes Providing Protection for Information Privacy 15
2. Privacy Act Record Systems Reported by Federal Agencies 23
3. Computerized and Manual Privacy Record Systems 23
4. Seriousness of Breaches of Confidentiality 29
5. Support for Potential Federal Laws on Information Abuse 31

Figures

Figure No. *Page*

1. Beliefs That Computers Are an Actual Threat to Personal Privacy in This Country 27
2. Change in Percent of Public Believing That Files Are Kept on Themselves 28
3. Percent of Public That Believes Each Agency "Shares" Information About Individuals With Others 30

Chapter 2

Electronic Record Systems and the Privacy Act: An Introduction

SUMMARY

Although privacy is a value that has always been regarded as fundamental, its meaning is often unclear. Privacy includes concerns about autonomy, individuality, personal space, solitude, intimacy, anonymity, and a host of other related concerns. There have been many attempts to give meaning to the term for policy purposes. In 1890, Samuel Warren and Louis Brandeis defined it as "the right to be let alone." In 1967, Alan Westin defined it as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." This latter definition served as the basis for the Privacy Act of 1974 (Public Law 93-579).

The Privacy Act was enacted by Congress to provide legal protection for and safeguards on the use of personally identifiable information maintained in Federal Government record systems. The Privacy Act established a framework of rights for individuals whose personal information is recorded, and the responsibilities of Federal agencies that collect and maintain such information in Privacy Act record systems.

When the Privacy Act was debated and enacted, Federal agency record systems were still based largely on paper documents. In 1986, many Federal agency record systems are based largely on electronic recordkeeping. Computers and telecommunications are used to process detailed information on millions of citizens. No longer is personal information merely stored in and retrieved from file cabinets; now large volumes of such information are collected, retrieved, disclosed, disseminated, manipulated, and disposed of by computers. Moreover, direct on-line linkages now make it possible to compare individual information with a host of public and private agencies. Computer tapes, software, and networking also make it possible to compare personal information stored in different record systems.

The Privacy Act, with the goal of providing the means by which individuals could control information about themselves, balanced the interests of Federal agencies in collecting and using personal information against the interests of individuals in controlling access to and use of that information. Technology has now altered that balance in favor of the agencies. Computers and telecommunication capabilities have expanded the opportunities for Federal agencies to use and manipulate personal information. For example, there has been a substantial increase in the matching of information stored in different databases as a way of detecting fraud, waste, and abuse, as will be discussed in chapter 3. Likewise, computers are increasingly being used to certify the accuracy and completeness of individual information before an individual receives a benefit, service, or employment, as will be discussed in chapter 4 on front-end verification. These technological capabilities appear to have outpaced the ability of individuals to protect their interests by using the mechanisms available under the Privacy Act.

In addition to technological threats to Privacy Act protections, several studies of the act's effectiveness have been critical of both agency implementation and Office of Management and Budget (OMB) oversight, and have questioned the individual's ability to use the remedies in a meaningful way. The technological changes have aggravated these problems, and have created some new ones as well.

OTA reached four general conclusions about individual privacy and electronic record systems that cut across all areas of information technology application:

1. **Advances in information technology are having two major, and somewhat opposing, effects on the electronic recordkeeping activities of Federal agencies.** They are facilitating electronic recordkeeping by Federal agencies, enabling them to process and manipulate more information with great speed. At the same time, the growth in the scale of computerization, the increase in computer networking and other direct linkages, the electronic searches of computerized files, and the proliferation of microcomputers are threatening Privacy Act protections.
2. **Federal agencies have invested only limited time and resources in Privacy Act matters.** Few staff are assigned to Privacy Act implementation, few agencies have developed agency-specific guidelines or updated guidelines in response to technological changes, and few have conducted record quality audits.
3. **Privacy continues to be a significant and enduring value held by the American public.** General concern over personal privacy has increased among Americans over the last decade, as documented by several public opinion surveys over the past 6 years. About one-half of the American public believes that computers are a threat to privacy, and that adequate safeguards to protect information about people are lacking. There is increasing public support for additional government action to protect privacy.
4. **The courts have not developed clear and consistent constitutional principles of information privacy, but have recognized some legitimate expectations of privacy in personal communications.**

An OTA survey of the use of information technology by Federal agencies revealed that:

- components within 12 cabinet-level departments and 13 independent agencies reported 539 Privacy Act record systems with 3.5 billion records. Forty-two percent of the systems were fully computerized, 18 percent were partially computerized, and 40 percent were manual. Of the large Privacy Act record systems (i.e., over 500,000 persons), 57 percent were fully computerized, 21 percent were partially computerized, and 22 percent were manual;[1]
- agencies responding reported an increase from a few thousand microcomputers in 1980 to about 100,000 in 1985;
- only about 8 percent of Federal agencies that responded have revised or updated their Privacy Act guidelines with respect to microcomputers; and
- only about 12 percent of agencies reported that they have conducted record quality audits.

INTRODUCTION

The Federal Privacy Act of 1974 was enacted by Congress to provide legal protection for and safeguards on the use of personally identifiable information maintained in Federal Government record systems. The Privacy Act established a framework of rights for individuals and responsibilities for Federal agencies that collect and maintain personally identifiable information. This framework incorporates a number of "fair information principles" including, primarily, that there should be no secret record systems, individuals should be able to see and correct their records, and information collected for one purpose should not be used for another.

---

[1] Agencies were asked to report only their 10 largest Privacy Act record systems. Twelve of thirteen cabinet departments responded (only the Department of Housing and Urban Development did not), as did 20 selected independent agencies. However, some major personal information collectors within cabinet departments (e.g., the Internal Revenue Service within the Department of the Treasury and the Departments of the Army and Navy within the Department of Defense) did not respond.

At the time the Privacy Act was debated, Federal agency record systems were still based largely on paper documents, with some agencies using large mainframe computers for the storage and retrieval of information in very large record systems. By 1986, Federal agencies have become electronic environments with computers and telecommunications being used to process detailed information on millions of citizens. Agencies now use computers, often microcomputers, to collect, disclose, disseminate, manipulate, and dispose of personal information. Direct on-line linkages between computerized databases make it possible to almost instantaneously compare information. Additionally, computer tapes and computer software make it possible to compare entire record systems.

The Privacy Act, with the goal of providing the means by which individuals could control personal information, balanced the interests of Federal agencies in collecting and using personal information against the interests of individuals in that information. Computer and telecommunication capabilities have expanded the interests of Federal agencies in personal information and enhanced their ability to process it. These capabilities have also overshadowed the ability of individuals to use the mechanisms available in the Privacy Act because, in general, it is more difficult for them to follow what occurs during the information-handling process.

The use of computers and telecommunications for processing personal information also offers opportunities for protecting that information. Techniques such as passwords, encryption, and audit trails are available to protect the confidentiality and security of information in an electronic environment. Although their use may provide more protection for the individual, these techniques do not necessarily give the individual control over the stages of information processing, as provided for in the Privacy Act.

BACKGROUND

Privacy

Privacy is a value that continues to be highly esteemed in American society, yet its meaning, especially for policy purposes, is often unclear. Privacy is a broad value, representing concerns about autonomy, individuality, personal space, solitude, intimacy, anonymity, and a host of other related concerns. There have been many attempts to define a "right to privacy." In a seminal article, Warren and Brandeis[2] defined it as "the right to be let alone." They found the primary source for a general right to privacy in the common law protection for intellectual and artistic property, and argued that:

> . . . the principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.

Subsequent legal debates have been structured by two points raised by Warren and Brandeis. The first is whether privacy is an independent value whose legal protection can be justified separately from other related interests, such as peace of mind, reputation, and intangible property. The second is controversy over their definition of the "right to privacy" as the "right to be let alone." Such a definition is so broad and vague that the qualifications necessary to make such a definition practical in society negate the right itself.

Second only to the Warren and Brandeis article in influence on the development of legal thinking regarding protection of privacy in the United States is Dean Prosser's 1960 *Califor-*

---

[2] "The Right to Privacy," *Harvard Law Review*, 1890.

nia Law Review article, "Privacy." His primary finding is that:

> At the present time the right of privacy, in one form or another is declared to exist by the overwhelming majority of the American courts.[3]

Prosser analyzed four distinct torts—intrusion, disclosure, false light, and appropriation—that could be isolated in State common law decisions and that represented four different types of privacy invasions. Each of these torts depends on physical invasion or requires publicity, and hence offers little protection for privacy of personal information. Although Prosser's analysis has received wide acceptance as a way of categorizing tort law relating to privacy, most legal scholars doubt that these traditional privacy protections in common law can, or should, be extended to cover more general privacy concerns.

In the mid-1960s, concern with the "privacy" of computerized personal information held by credit agencies and the government rekindled interest in defining a right to privacy. Edward Shils viewed privacy of personal information as:

> . . . a matter of the possession and flow of information. . . Privacy in one of its aspects may therefore be defined as the existence of a boundary through which information does not flow from the persons who possess it to others.[4]

Alan Westin conceived of privacy as "an instrument for achieving individual goals of self-realization," and defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[5]

The "right to privacy" as "the right to control information about oneself" has served as the definition for policy purposes in the United States. Various statutes have been designed to give individuals the means to control information about themselves. Such means include primarily the right to know and the right to challenge and correct. Organizations are also expected to follow "Principles of Fair Information Use,"[6] which establish standards and regulations for collection and use of personal information. See table 1 for a list of statutes providing protection for information privacy.

History of the Privacy Act

In the mid-1960s, Congress and certain executive agencies began to study the privacy implications of records maintained by Federal agencies. The congressional concern with privacy and individual records was precipitated by the 1965 Social Science Research Council proposal that the Bureau of the Budget establish a National Data Center to provide basic statistical information originating in all Federal agencies.

In 1966, the Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure[7] and the House Committee on Government Operations, Special Subcommittee on Invasion of Privacy,[8] held hearings on the proposals for a National Data Center. Both committees were unconvinced of the need for such a center or of its ability to keep data confidential. In 1967 and 1968, the House and Senate again held hearings on the proposal for a National Data Center, and remained unconvinced that such a center could adequately protect the privacy of individual records. The committees and various witnesses feared that once such a center was established, its limited role would not be maintained. There was also great reluctance to condone the centralization of both personal information and responsibility for that information within an executive agency. Although the committees agreed that the existing situation was inefficient, they believed that such decentralized inefficiency was amenable to congressional oversight, whereas centralized efficiency would be more difficult to check. The proposal for a National Data Center was therefore rejected.

---

[3] William L. Prosser, "Privacy," *California Law Review*, vol. 48, 1980, pp. 383, 386.

[4] Edward Shils, "Privacy: Its Constitution and Vicissitudes," *Law and Contemporary Problems*, vol. 31, 1966, pp. 281, 282.

[5] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 39.

[6] A "Code of Fair Information Practice" was first developed in: U.S. Department of Heath, Education, and Welfare, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[7] See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasions of Privacy* (Government Agencies), Hearings, 89th Cong., February 1965, June 1966 (Washington, DC: U.S. Government Printing Office, 1965-67).

[8] See U.S. Congress, House Committee on Government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and Invasion of Privacy*, Hearings, 89th Cong., 2d sess., July 25, 27, 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966).

In 1970, the Senate Judiciary Committee, Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, Jr., began a 4-year study of Federal Government databanks containing personal information and held related oversight hearings.[9] These hearings and the survey of agencies conducted by the Ervin Subcommittee laid the groundwork for the Privacy Act of 1974.

In 1972, Alan Westin and Michael Baker, with the support of the Russell Sage Foundation and the National Academy of Sciences, released a report, *Databanks in a Free Society*, in which they concluded that computerization of records was not the villain it had often been portrayed to be. Their policy recommendations applied to both computerized and manual systems and included:

1. a "Citizen's Guide to Files";
2. rules for confidentiality and data sharing;
3. limitations on unnecessary data collection;
4. technological safeguards;
5. restricted use of the social security number; and
6. the creation of information trust agencies to manage sensitive data.[10]

Table 2-1.—Statutes Providing Protection for Information Privacy

Fair Credit Reporting Act of 1970 (Public Law 91-508, 15 U.S.C. 1681) requires credit investigation and reporting agencies to make their records available to the subject, provides procedures for correcting information, and permits disclosure only to authorized customers.

Crime Control Act of 1973 (Public Law 93-83) requires that State criminal justice information systems, developed with Federal funds, be protected by measures to insure the privacy and security of information.

Family Educational Rights and Privacy Act of 1974 (Public Law 93-380, 20 U.S.C. 1232(g)) requires schools and colleges to grant students or their parents access to student records and procedures to challenge and correct information, and limits disclosure to third parties.

Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. 552(a)) places restrictions on Federal agencies' collection, use, and disclosure of personally identifiable information, and gives individuals rights of access to and correction of such information.

Tax Reform Act of 1976 (26 U.S.C. 6103) protects confidentiality of tax information by restricting disclosure of tax information for nontax purposes. The list of exceptions has grown since 1976.

Right to Financial Privacy Act of 1978 (Public Law 95-630, 12 U.S.C. 3401) provides bank customers with some privacy regarding their records held by banks and other financial institutions, and provides procedures whereby Federal agencies can gain access to such records.

Privacy Protection for Rape Victims Act of 1978 (Public Law 95-540) amends the Federal Rules of Evidence to protect the privacy of rape victims.

Protection of Pupil Rights of 1978 (20 U.S.C. 1232(h)) gives parents the right to inspect educational materials used in research or experimentation projects, and restricts educators from requiring intrusive psychiatric or psychological testing.

Privacy Protection Act of 1980 (Public Law 96-440, 42 U.S.C. 2000(a)(a)) prohibits government agents from conducting unannounced searches of press offices and files if no one in the office is suspected of committing a crime.

Electronic Funds Transfer Act of 1978 (Public Law 95-630) provides that any institution providing EFT or other bank services must notify its customers about third-party access to customer accounts.

Intelligence Identities Protection Act of 1982 (Public Law 97-200) prohibits the unauthorized disclosure of information identifying certain U.S. intelligence officers, agents, informants, and sources.

Debt Collection Act of 1982 (Public Law 97-365) establishes due process steps (notice, reply, etc.) that Federal agencies must follow before they can release bad debt information to credit bureaus.

Cable Communications Policy Act of 1984 (Public Law 98-549) requires the cable service to inform the subscriber of: the nature of personally identifiable information collected and the nature of the use of such information; the disclosures that may be made of such information; the period during which such information will be maintained; and the times during which an individual may access such information. Also places restrictions on the cable services' collection and disclosures of such information.

Confidentiality provisions are included in several statutes, including: the Census Act (13 U.S.C. 9214), the Social Security Act (42 U.S.C. 408(h)), and the Child Abuse Information Act (42 U.S.C. 5103(b(2)(e))).

NOTE: All statutes embody the same scheme of individual rights and fair information practices.

SOURCES: Robert Aldrich, *Privacy Protection Law in the United States* (NTIA Report 82-98, May 1982); Sarah P. Collins, *Citizens Control Over Records Held by Third Parties* (CRS Report No. 78-255, Dec. 8, 1978); and the Office of Technology Assessment.

---

[9] See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks, Computers and the Bill of Rights*, Hearings, 92d Cong., 1st sess., Feb. 24-25 and Mar. 2, 3, 4, 9, 10, 11, 15, and 17, 1971, parts I and II (Washington, DC: U.S. Government Printing Office, 1971).

[10] Alan F. Westin and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle/The New York Times Book Co., 1972).

In 1973, the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems released its report, *Records, Computers and the Rights of Citizens,* in which it discussed three changes resulting from the use of computerized recordkeeping:

1. an increase in organizational data processing capacity;
2. more access to personal data; and
3. the creation of a class of technical recordkeepers.

It recommended the enactment of a Federal "Code of Fair Information Practice" that would apply to both computerized and manual systems. This code served as the model for the Privacy Act, as well as for the Council of Europe's 1974 "Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector."[11] The major principles of the code include:

- There must be no personal data recordkeeping system whose very existence is secret.
- There must be a way for an individual to find out what information about him or her is in a record and how it is used.
- There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[12]

In 1974, in the wake of Watergate, hearings on numerous privacy bills were held in both the Senate and the House.[13] In the subcommittee hearings, there was little disagreement on the need for individual rights with respect to personal information held by Federal agencies. Discussions centered instead on the logistics of enabling individuals to use these rights, and the specific fair information practices that agencies were to follow. The Senate version also provided for a permanent Federal Privacy Board with regulatory powers, while the House version provided no such oversight mechanism. As a compromise, the Privacy Protection Study Commission was created, and oversight responsibilities were given to the Office of Management and Budget.

In 1977, the Privacy Protection Study Commission released its comprehensive report, *Personal Privacy in an Information Society,* which analyzed the policy implications of personal recordkeeping in a number of areas including credit, insurance, employment, medical care, investigative reporting, education, and State and local government.[14] The report made numerous policy recommendations, very few of which have been realized in statutory law.

Implementation of the Privacy Act

A number of studies have evaluated the implementation and effectiveness of the Privacy Act. Most notable are analyses done by the House Committee on Government Operations, the Privacy Protection Study Commission, and the General Accounting Office.[15] All conclude that the act has been disappointing in providing protection for individuals from misuse of personal information by Federal agencies. For example, the Privacy Protection Study Commission reached three general conclusions:

---

[11] Reprinted in *Privacy and Protection of Personal Information in Europe,* Staff Report of the Senate Committee on Government Operations (Washington, DC: U.S. Government Printing Office, March 1975).

[12] U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[13] See U.S. Congress, Senate Committee on Government Operations, Ad Hoc Subcommittee on Privacy and Information Systems, and Committee on the Judiciary, Subcommittee on Constitutional Rights, *Privacy—The Collection, Use and Computerization of Personal Data,* Joint Hearings, 93d Cong., 2d sess., June 18-20, 1974 (Washington, DC: U.S. Government Printing Office, 1974).

[14] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington DC: U.S. Government Printing Office, 1977) with five appendices: *Privacy Law in the State; The Citizen as Taxpayer; Employment Records; The Privacy Act of 1974: An Assessment; and Technology and Privacy.*

[15] See U.S. Congress, House Committee on Government Operations, Government Information and Individual Rights Subcommittee, *Implementation of the Privacy Act of 1974: Databanks* (1975); Privacy Protection Study Commission, *The*

1. the Privacy Act represents a large step forward, but it has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect;
2. agency compliance with the act is difficult to assess because of the ambiguity of some of the act's requirements, but, on balance, it appears to be neither deplorable nor exemplary; and
3. the act ignores or only marginally addresses some personal-data recordkeeping policy issues of major importance now and for the future.[16]

In his opening statement before hearings on oversight of the Privacy Act, Representative Glenn English, Chairman of the Subcommittee on Government Information, Justice, and Agriculture of the Committee on Government Operations, remarked that:

> One of my chief concerns is that the bureaucracy, with the approval of OMB, has drained much of the substance out of the Act. As a result, the Privacy Act tends to be viewed as strictly a procedural statute. For example, agencies feel free to disclose personal information to anyone as long as the proper notices have been published in the Federal Register. No one seems to consider any more whether the Privacy Act prohibits a particular use of information.[17]

All of the studies evaluating the implementation and effectiveness of the Privacy Act cite its major weaknesses to be its reliance on individual initiative; the ambiguity of some of the act's requirements; the casual manner in which OMB has implemented and enforced the act; and OMB guidelines issued subsequent to the act that seem to contradict the purpose of the act. These studies report that the act has been used less than anticipated. This is attributed to the investment of time and money an individual must make, and to the finding that agencies have not made it easy to use the Privacy Act.

The purpose of the Privacy Act is "to provide certain safeguards for an individual against an invasion of privacy" [Public Law 93-579, sec. 2(b)]. To this end, the act stipulates that Federal agencies meet six major requirements. Each of these requirements, and agency experience to date in meeting each requirement, is discussed below.

Requirement 1

Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies.

To this end, agencies are to publish in the *Federal Register* an annual notice of the existence and character of all systems of records containing personal information, and a notice of any new systems of records or new uses of the information in an existing system. The purpose of this was to ensure that there were no secret systems of records by giving the individual notice of agency recordkeeping practices. However, most agree that the *Federal Register* is not the ideal vehicle for such notice as it is not easily accessible to most people. In "The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974" for calendar years 1982 and 1983, OMB identified the effectiveness of the public notice process as one area for further study, noting that:

> The problem may lie in the method used to disseminate this kind of information. While the *Federal Register* stands as the official organ of the government, it is a publication with limited circulation read by few ordinary citizens.[18]

Privacy Act of 1974: An Assessment (1977); General Accounting Office, *Agencies' Implementation of and Compliance With the Privacy Act Can Be Improved* (1978); and House Committee on Government Operations, Government Information, Justice, and Agriculture Subcommittee, *Oversight of the Privacy Act of 1974* (1983).

[16] Privacy Protection Study Commission, app. 4, op. cit., p. 77.

[17] House Committee on Government Operations, 1983, op. cit., p. 5.

[18] "The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974," CY 1982-1983 (issued Dec. 4, 1985), p. 118.

In 1983, OMB, on the basis of the Congressional Reports Elimination Act of 1982 (Public Law 97-375), eliminated the requirement that agencies republish all of their system notices each year in the *Federal Register*. The reason offered for this decision was lack of public and congressional interest. OMB viewed agency republication as a duplication of the *Federal Register's* annual compilation of Privacy Act notices. OMB recently estimated that the elimination of this requirement, including its administrative expenses, had saved the government over $1 million.[19]

Additionally, the Privacy Act requires agencies to inform individuals, on an application form or on a separate form that individuals can retain, of the following information: 1) the authority that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; 2) the principal purpose or purposes for which the information is intended to be used; 3) the routine uses that may be made of the information; and 4) the effects of not providing all or any part of the requested information [see Public Law 93-579, sec. 3(e)(3)]. See box A for an example of a Privacy Act notice.

Requirement 2

Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent.

To this end, agencies are to acquire the prior written consent of the individual to whom the record pertains before disclosing a record *unless* one of *twelve* exceptions is met [see Public Law 93-579, sec. 3(b)]. Included in this list are the releases of information to: 1) those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties; 2) the Bureau of the Census for census-related activities; 3) the National Archives of the United States for historical preservation; 4) a government agency for a civil or criminal law enforcement activity; 5) either House of Congress; and 6) the Comptroller General. The Debt Collection Act of 1982 added an exception for agency disclosure of bad debt information to credit bureaus.

Additionally, an agency may disclose a record without the consent of the individual if the disclosure would be for a "routine use," defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" [Public Law 93-579, sec. 3(a)(7)]. If an agency intends to disclose personal information for a "routine use," then it must publish a notice in the *Federal Register*. This exemption has proved to be quite controversial. In the 1983 Oversight of the Privacy Act Hearings, James Davidson, former counsel to the Senate Subcommittee on Intergovernmental Relations of the Committee on Government Operations, stated that the "routine use" exemption was:

> . . . designed to require that the agencies examine the data, see if the use that the other agency was going to put it to was compatible with the reason for which it was collected, then issue notice so the public and other agencies and OMB could comment on the propriety of the exchange.[20]

Davidson went on to note that this has not been the way that agencies have used the routine use exemption; rather, if agencies had been routinely exchanging information over the years, they have assumed that the routine use exemption allows them to continue.

There have been a number of legislative proposals to amend the "routine use" definition. The Privacy Protection Study Commission recommended that, in addition to the requirement that the use of a record be "compatible with the purposes for which it was collected," the use also be "consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained."[21] In the 1982

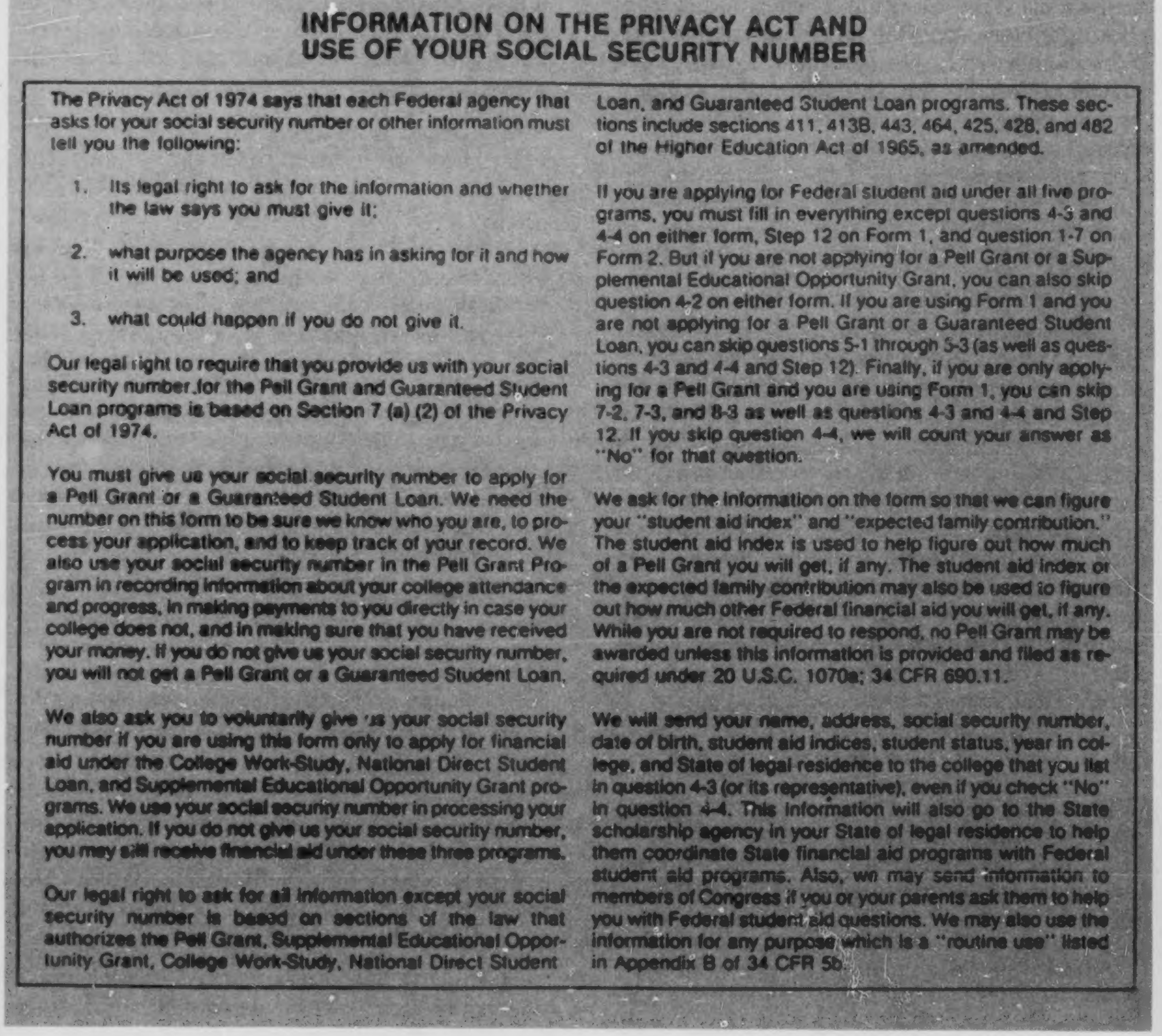
---

[19] Ibid., p. 10.

[20] House Committee on Government Operations, 1983, op. cit., p. 51.

[21] Privacy Protection Study Commission, app. 4, op. cit., p. 120.

Box A.—U.S. Department of Education Application for Federal Student Aid, 1986-87 School Year



INFORMATION ON THE PRIVACY ACT AND
USE OF YOUR SOCIAL SECURITY NUMBER

The Privacy Act of 1974 says that each Federal agency that asks for your social security number or other information must tell you the following:

1. Its legal right to ask for the information and whether the law says you must give it;
2. what purpose the agency has in asking for it and how it will be used; and
3. what could happen if you do not give it.

Our legal right to require that you provide us with your social security number for the Pell Grant and Guaranteed Student Loan programs is based on Section 7 (a) (2) of the Privacy Act of 1974.

You must give us your social security number to apply for a Pell Grant or a Guaranteed Student Loan. We need the number on this form to be sure we know who you are, to process your application, and to keep track of your record. We also use your social security number in the Pell Grant Program in recording information about your college attendance and progress, in making payments to you directly in case your college does not, and in making sure that you have received your money. If you do not give us your social security number, you will not get a Pell Grant or a Guaranteed Student Loan.

We also ask you to voluntarily give us your social security number if you are using this form only to apply for financial aid under the College Work-Study, National Direct Student Loan, and Supplemental Educational Opportunity Grant programs. We use your social security number in processing your application. If you do not give us your social security number, you may still receive financial aid under these three programs.

Our legal right to ask for all information except your social security number is based on sections of the law that authorizes the Pell Grant, Supplemental Educational Opportunity Grant, College Work-Study, National Direct Student Loan, and Guaranteed Student Loan programs. These sections include sections 411, 413B, 443, 464, 425, 428, and 482 of the Higher Education Act of 1965, as amended.

If you are applying for Federal student aid under all five programs, you must fill in everything except questions 4-3 and 4-4 on either form, Step 12 on Form 1, and question 1-7 on Form 2. But if you are not applying for a Pell Grant or a Supplemental Educational Opportunity Grant, you can also skip question 4-2 on either form. If you are using Form 1 and you are not applying for a Pell Grant or a Guaranteed Student Loan, you can skip questions 5-1 through 5-3 (as well as questions 4-3 and 4-4 and Step 12). Finally, if you are only applying for a Pell Grant and you are using Form 1, you can skip 7-2, 7-3, and 8-3 as well as questions 4-3 and 4-4 and Step 12. If you skip question 4-4, we will count your answer as "No" for that question.

We ask for the information on the form so that we can figure your "student aid index" and "expected family contribution." The student aid index is used to help figure out how much of a Pell Grant you will get, if any. The student aid index or the expected family contribution may also be used to figure out how much other Federal financial aid you will get, if any. While you are not required to respond, no Pell Grant may be awarded unless this information is provided and filed as required under 20 U.S.C. 1070a; 34 CFR 690.11.

We will send your name, address, social security number, date of birth, student aid indices, student status, year in college, and State of legal residence to the college that you list in question 4-3 (or its representative), even if you check "No" in question 4-4. This information will also go to the State scholarship agency in your State of legal residence to help them coordinate State financial aid programs with Federal student aid programs. Also, we may send information to members of Congress if you or your parents ask them to help you with Federal student aid questions. We may also use the information for any purpose which is a "routine use" listed in Appendix B of 34 CFR 5b.

and 1983 "President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974," problems with the interpretation and implementation of the "routine use" disclosure were identified as Privacy Act issues for further study. The "Annual Report" stated that it would "be useful for the Congress to reconsider this problem and provide clearer guidance on routine use disclosures."[22]

Requirement 3

Permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records.

These individual rights are a cornerstone of the act; however, they have not been used as much as anticipated. Reasons offered include:

1. the time an individual must spend in communicating with an agency;

---

[22] "The President's Annual Report," 1982-1983, op. cit., p. 121.

2. the possible difficulty in adequately identifying personal records for which access is requested; and
3. the lack of public awareness of these rights.

The Privacy Protection Study Commission concluded that:

> Agency rules on individual access, and on the exercise of the other rights the Act establishes, appear, in most instances, to be in compliance with the Act's rule-making requirements. Yet, they too are often difficult to comprehend, and because the principal places to find them are in the *Federal Register* and the *Code of Federal Regulations*, it is doubtful that many people know they exist, let alone how to locate and interpret them.[23]

An additional reason that this goal has not been realized is that there are seven exemptions to this requirement that are authorized by the Privacy Act itself. In general, these exemptions include those systems of records that include investigatory material compiled for law enforcement purposes or for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or promotion, military service, Federal contracts, or access to classified material. Also exempt are those systems of records that are maintained in connection with providing protective services to the President or other individuals, and those that are required by statute to be maintained and used solely as statistical records [Public Law 93 579, sec. 3(k)].

In the 1979 "Annual Report of the President on the Implementation of the Privacy Act of 1974," the individual access provisions were described as the "most apparently successful provision of the Act."[24] It was reported that since 1977, agencies had recorded over 2 million requests for access and had complied with over 96 percent of the requests. But, the 1979 Annual Report noted that it was not clear whether the access requests were the "direct result of the Act" because of prior procedures by which employees and clients were given access to their records.[25] In the 1982-83 Annual Report, OMB reported that access requests and requests to amend records had declined for most of the agencies with major record holdings. OMB attributed this to the existence of other agency access policies (for example, for personnel records) that are used rather than filing a Privacy Act request.[26]

Requirement 4

Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

These "Fair Information Principles" are another cornerstone of the act. Yet, the agencies have loosely construed these requirements and have at times ignored them altogether. The Privacy Protection Study Commission concluded that:

> None of these several collection requirements and prohibitions appears to have had a profound impact on agency record-keeping practice, mainly because they are either too broadly worded or have been perceived as nothing more than restatements of longstanding agency policy.[27]

In testimony before the House Subcommittee on Government Information, Justice, and Agriculture, John Shattuck, then legislative director for the American Civil Liberties Union, reached a similar conclusion, stating that:

> The Code of Fair Information Practices which constitutes the core of the statute is so general and abstract that it has become little more than precatory in practice, and has proved easy to evade.[28]

The vagueness of the principles contributes to agencies' practices. The act does not define, nor does it require agencies to set standards for, such terms as "current" or "necessary." The act also does not develop, nor does it require agencies to develop, procedures to ensure "accurate" information or "adequate safeguards . . . to prevent misuse."

---

[23] Privacy Protection Study Commission, app. 4, op. cit., p. 84.

[24] "Fifth Annual Report of the President on the Implementation of the Privacy Act of 1974," Calendar Year 1979 (released August 1980), p. 11.

[25] Ibid.

[26] Ibid., p. 20.

[27] Privacy Protection Study Commission, app. 4, op. cit., p. 44.

[28] House Committee on Government Operations, 1983, op. cit., p. 273.

Requirement 5

Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority.

As discussed above, the exemptions for permission to disclose, and for access and correction, are broadly defined. However, overall, agencies exempt only a small percentage of their systems of records. In order to ensure that agencies only exempted systems of records where necessary, the Privacy Act requires that the President report annually on the operation of the exemption provision. In the 1979 Annual Report, OMB concluded that agencies have "implemented this provision in a thoughtful and sparing manner" and that:

- Only 14 percent of total systems have been exempted.
- Agencies have invoked exemptions to completely deny access in only 0.2 percent of cases.
- Agencies routinely screen records in exempt systems and release material not deemed to need protection.[29]

In the 1982-83 Annual Report, OMB reported that, from 1975 to 1983, the number of exempt systems declined by over 16 percent.[30]

Requirement 6

Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

This requirement is intended to provide individuals the means to enforce agencies to comply with the provisions of the act, if they were not satisfied with the outcome of an administrative appeal. The time and cost involved to bring a suit under the Privacy Act is often prohibitive. In addition, some individuals have used the Freedom of Information Act, rather than the Privacy Act, to gain access to their records, and thus cannot bring suit under the Privacy Act. Where individuals have used the Privacy Act, their civil suits have rarely been successful because of the need to find "willful or intentional" activity, because injunctive relief under the act is unclear, and because the courts have narrowly construed the circumstances under which an individual can recover damages.[31] Richard Ehlke of the Congressional Research Service summarized the situation as follows:

> Despite over seven years of operation, the case law under the Privacy Act is relatively undeveloped. The greater visibility of the Freedom of Information Act, the breadth of many of the Privacy Act exceptions, and the limited remedial scheme of the Act are undoubtedly factors in this development. Much of the litigation has focused on these aspects of the Act—the limitations inherent in the "record" and "system of records" triggers to the Act; the expansive law enforcement exemptions; the exceptions to the consensual disclosure requirement; and the limited remedies available to redress many violations of the Act.[32]

---

[29] "President's Annual Report, 1979," op. cit., p. 14.

[30] "President's Annual Report, 1982-83," op. cit., p. 19.

[31] See Richard Ehlke, "Litigation Trends Under The Privacy Act," June 1983, *Congressional Research Service*, in *Oversight of the Privacy Act of 1974*, op. cit., pp. 437-469.

[32] Ibid., pp. 468-469.

FINDINGS

OTA has reached four general conclusions about individual privacy and electronic record systems that cut across all areas of application of information technology. Each finding is discussed below.

Finding 1

Advances in information technology are having two major, and somewhat opposing, effects on the electronic recordkeeping activities of Federal agencies.

They are facilitating electronic recordkeeping by Federal agencies, enabling them to process and manipulate more information with great speed. At the same time, the growth in the scale of computerization, the increase in computer networking and other direct linkages, electronic searches of computerized files, and the proliferation of microcomputers are threatening Privacy Act protections.

In the early 1960s, the use of computers to process personal information in Federal agencies was in its beginning stages and Federal agencies were still largely paper environments.[33] At this time, most computing was done on large mainframes by central processing, and only record systems containing a large number of records were stored on computers. In 1975, the First Annual Report of the President on Implementation of the Privacy Act reported that 73 percent of the personal data systems subject to the act were totally manual, but the remaining 27 percent that were fully or partially computerized contained over 80 percent of the total individual records.[34]

In 1985, the increase in the number of computerized records is significant. In the OTA survey, agencies were asked to report their 10 largest Privacy Act record systems. Components within 12 cabinet-level departments[35] and 13 independent agencies[36] reported a total of 539 Privacy Act record systems containing 3.5 billion records. Of these systems, 42 percent were totally computerized, 18 percent were partially computerized, and 40 percent were wholly manual (see table 2). More importantly, of the large systems of records (i.e., over 500,000 persons), 57 percent were totally computerized, 21 percent were partially computerized, and 22 percent were wholly manual (see table 3).

The qualitative changes that have occurred in the various stages of the information process as a result of computerization are also significant. No longer is information merely stored and retrieved by computer. Now information is routinely collected on computer tapes, used within an agency in computer form, exchanged with and disclosed to regional offices or other agencies in computer form, manipulated and analyzed with sophisticated computer software, and archived on computer tapes.

---

[33] Before the Privacy Act was passed, two surveys of the degree of computerization of Federal agency record systems were conducted. In 1966, the Senate Judiciary Subcommittee on Administrative Practice and Procedure conducted a survey of "government dossiers" to determine the extent and nature of Federal agencies' collection of personal information. The subcommittee determined that Federal files contained more than 3 billion records on individuals, and that over one-half of these records were retrievable by computers. [See: U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Government Dossier* (Committee Print) (Washington, DC: U.S. Government Printing Office, 1967), pp. 7-9.] The Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, surveyed agencies and found that 86 percent of the 858 databanks with 1.25 billion records on individuals were, at least in part, computerized. The large percentage of computerization found by the Ervin study may be attributed in part to the fact that the study used the phrase "databank containing personal information about individuals." To many, "databank" may imply a computerized system; thus, it is likely that manual systems were underreported in the Ervin survey. (See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks and Constitutional Rights,* 93d Cong., 2d sess., 1974.)

[34] *Federal Personal Data Systems Subject to the Privacy Act of 1974, First Annual Report of the President, Calendar Year 1975,* pp. 4-6.

[35] Only the Department of Housing and Urban Development did not respond to this question at all. However, some major personal information collectors within cabinet departments (e.g., Internal Revenue Service within the Department of the Treasury and the Departments of the Army and Navy within DOD) did not respond.

[36] Consumer Product Safety Commission, Federal Trade Commission, National Aeronautics and Space Administration, Nuclear Regulatory Commission, Securities and Exchange Commission, Selective Service System, Agency for International Development, Federal Election Commission, Federal Reserve System, Small Business Administration, National Archives and Records Administration, Commission on Civil Rights, and Arms Control and Disarmament Agency.

Table 2.—Privacy Act Record Systems Reported by Federal Agencies[a]

Agency	Fully computerized		Partially computerized		Subtotals		Manual		Totals	
	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records
Agriculture	22	27.0[b]	6	1.5	28	28.5	14	0.5	42	29.0
Commerce	13	882.1	3	0.4	16	882.5	5	1.4	21	883.9
DOD	15	50.0	4	1.7	19	51.7	32	3.6	51	55.3
Education	3	1.7	1	0.0	4	1.7	0	0.0	4	1.7
Energy	3	0.4	7	0.4	10	0.8	4	0.3	14	1.5
DHHS	26	1,304.6	16	9.0	42	1,313.6	20	90.1	62	1,403.7
Interior	32	4.5	11	5.2	43	9.7	17	0.4	60	10.1
Justice	28	101.2	9	224.4	37	325.6	31	2.2	68	327.8
Labor	8	1.6	9	0.9	17	2.5	1	0.0	18	2.5
DOT	36	10.0	8	3.0	44	13.0	17	0.2	61	13.2
Treasury	16	48.8	6	36.1	22	84.9	20	460.3	42	545.2
State	0	0.0	1	20.0	1	20.0	9	90.2	10	110.2
Independent agencies	27	22.4	15	1.0	42	23.4	44	51.4	86	74.8
Totals	229	2,454.3	96	303.6	325	2,757.9	214	700.6	539	3,458.9

[a] Agencies were asked to report only their 10 largest Privacy Act record systems. Twelve of thirteen cabinet departments responded (only the Department of Housing and Urban Development did not), as did 13 out of 20 independent agencies (see app. B at the end of this report for a list) and some major privacy recordholders did not respond (e.g., the Internal Revenue Service in the Department of the Treasury and the Departments of Army and Navy in the Department of Defense).

[b] Millions of records.

SOURCE: Office of Technology Assessment.

Table 3.—Computerized and Manual Privacy Record Systems

	Large systems[a]		Medium systems[b]		Small systems[c]		Totals	
	Number	Number of persons	Number	Number of persons	Number	Number of persons	Number	Number of persons
100% computerized	43	1,653,336,199	105	11,277,938	81	237,240	229	1,664,851,377
Partially computerized	16	285,880,382	41	3,912,622	39	213,790	96	290,006,794
100% manual	17	695,419,523	50	5,015,434	147	327,666	214	700,762,623

[a] Over 500,000 persons.

[b] 10,001 to 500,000 persons.

[c] Under 10,000 persons.

SOURCE: Office of Technology Assessment.

Another significant change is the direct linkage of computer records via telecommunication systems. This allows for easy disclosure and exchange of information. On-line access can occur, for example, via private or public telephone lines or through local networks within an agency. One factor supporting the transition of Federal information systems to direct linkages is cost—the cost of a typical network interface was $500 in 1982, but is expected to drop to about $50 by 1987.[37] Another factor is the ease and efficiency to an agency official of communicating directly with the computer as information is collected or needed, rather than compiling transactions, batch-processing them on a tape at the end of the day or week, and waiting for a reply.

With such computer networking, the exchanges of information occur rapidly, often leaving no audit trail of who had access to the data or what changes were made. Monitoring the use of agency information becomes much more difficult in this environment. But, at the same time, the environment supports a vast increase in the exchange and manipulation of information, as well as an increase in the number of people having access to the information. In 1977, the Privacy Protection Study Commission warned that:

> The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.[38]

---

[37] See Michael Killen, "The Microcomputer Connection to Local Networks," *Data Communications*, December 1982.

[38] Privacy Protection Study Commission, app. 4, op. cit., p. 108.

Another technological development that has implications for Privacy Act protections is efficient electronic searching through computer records. The two most common types of searches are computer matching and computer profiling (or computer screening). In a computer match, two sets of computer files are compared record by record to look for any individuals who appear in both files. In a computer profile or computer screen, a single computer file is searched for selected factors about a specific type of individual. Because of the importance of these electronic searches, each will be discussed in depth in the following chapters.

Another critical factor in the Federal agency technology environment in the mid-1980s is the microcomputer. The microcomputer puts the power of information collection, storage, retrieval, exchange, manipulation, and printing into the hands of discrete individuals. In doing so, it raises privacy, security, productivity, and management issues that had been irrelevant or dormant in other eras of information processing.[39]

Because of the control over information processing that microcomputers give users and because of their relatively low cost, the use of microcomputers has grown dramatically across all sectors of society. The Federal Government has not been immune to this trend. All agencies are experiencing an influx of microcomputers. The OTA survey revealed that the agencies surveyed had a few thousand microcomputers in 1980 and over 100,000 in 1985.

A major impetus in this demand for microcomputers within the Federal Government is the perceived need to increase productivity and efficiency. The broad range of information processing features that a microcomputer offers and the variety of software programs available make microcomputers attractive throughout an agency. For clerical work, microcomputers are used most often for document preparation and data entry.[40] At the administrative level, microcomputers are used for accounting, budgeting, and planning. Microcomputers can be used by professionals for data analysis as well as document preparation. For technical users, microcomputers offer control over system design and programming.[41]

Microcomputers complicate the monitoring of the uses of personal information for two reasons. First, they make it easier for individual users to create their own systems of records. This complicates Privacy Act oversight because files created on microcomputers were not considered when the Privacy Act was enacted, and it may be impractical to subject them to the act. The Privacy Act applies to a "record" that is retrieved from a "system of records." The Privacy Act defines "record" to mean:

> . . . any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

The act defines "system of records" to mean:

> . . . a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[42]

If a file created and maintained on a microcomputer meets the criteria for a system of records, i.e., is retrieved by name, identifier, or other identifying particular, then individuals should have the right to access and amend their records. To do so, all microcomputer files containing records that are retrievable by name or other identifier would need to be reported to the Privacy Act Officer and noted in the *Federal Register.*

---

[39] The KBL Group, Inc., "Agency Profiles of Civil Liberties Practices," OTA contractor report, December 1984, p. 153.

[40] See U.S. Congress, Office of Technology Assessment, *Automation of America's Offices*, OTA-CIT-287 (Washington, DC: U.S. Government Printing Office, December 1985) for an in-depth analysis of the effects of microcomputers in the workplace.

[41] National Bureau of Standards, *Microcomputers: Introduction to Features and Uses*, Special Publication 500-110, March 1984, pp. viii-ix.

[42] Privacy Act of 1974 (Public Law 93-579), sec. 3(a)(4)(5).

The second feature of the microcomputer that makes it difficult to monitor the uses of personal information is that a microcomputer serves as a remote terminal to access centralized systems of records. Such shifting of data from mainframes to microcomputers raises critical questions of data integrity and security. For example, when a record is being used by one user, there may be no other access to that information. More importantly, there may be no audit trail of additions and deletions.[43] Additionally, there may be no indication of how current the records are, thus increasing the likelihood that inaccurate data will be disseminated.[44]

At the present time, most microcomputers in Federal agencies are desk-top models. The trend to portable computers—also known as briefcase, lap, or notebook computers—and transportable computers will aggravate the problems of data integrity and security, especially since information will be transported out of government offices into areas that are neither controlled nor secured. Another technological development that will have implications for the processing of personal information is the multiuser microcomputers, or "super microcomputers," which are used primarily for group work situations.

Finding 2

Federal agencies have invested only limited time and resources in Privacy Act matters. Few staff are assigned to Privacy Act matters, few agencies have developed agency-specific guidelines or updated guidelines in response to technological changes, and few have conducted record quality audits.

The Privacy Act allows agencies much latitude to develop their own arrangements for supervising implementation and compliance with the act. The only requirement the act places on agencies is to:

> . . . establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance [Public Law 93-579, sec. 3(e)(9)].

In 1977, the Privacy Protection Study Commission reviewed agency experience and concluded that:

> . . . the 97 Federal agencies that maintain systems of records subject to the Privacy Act of 1974 have all taken different approaches to administration, training, and compliance monitoring . . . agencies or components of agencies that have carefully structured programs for administering the Act appear to be the ones in which the Act's objectives are being best achieved.[45]

Based on responses to the OTA survey of Federal agencies, 67 percent of agencies responding reported one (34 agencies) or less than one (33 agencies) full-time equivalent (FTE) staff assigned to Privacy Act matters. Only seven agencies reported ten or more FTEs assigned to Privacy Act matters, and six of these were located in the Department of Justice. The FBI reported the largest number of FTEs—65—assigned to Privacy Act issues.

The Privacy Act requires agencies to:

> . . . maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination [Public Law 93-579, sec.3(e)(5)].

OTA asked agencies to specify the procedures they follow to ensure Privacy Act record quality (for example, complete and accurate records). In response, most agencies submitted a copy of their policy directives containing general information and procedures for administering the Privacy Act. Only about 24 percent (30 agencies) have developed agency-specific guidelines or procedures for determining what is "relevant" and "timely" information within their agency.

---

[43] National Bureau of Standards, op. cit., p. 96.

[44] The KBL Group, Inc., op. cit., p. 162.

[45] Privacy Protection Study Commission, app. 4, op. cit., p. 108.

The results of the OTA survey also indicated that few agencies had conducted audits of record quality. Of 127 agency respondents, only about 13 percent (16 agencies) indicated that they conducted record quality audits. Of these 16 agencies, none provided copies of the results.[46] With respect to record quality statistics for law enforcement, investigative, and intelligence record systems, only one agency provided statistics (for three systems under its jurisdiction). No statistics were provided for any of the other 82 systems reported.[47]

The OTA survey also asked whether agencies had revised or updated Privacy Act guidelines with respect to microcomputers. Of 119 agency respondents, only 8.4 percent (10 agencies) had done so. One agency noted that microcomputers were not used in connection with the maintenance of Privacy Act information; however, as was noted above, files on microcomputers or accessible through microcomputers may well fall under the Privacy Act "system of records" criteria.

Finding 3

Privacy continues to be a significant and enduring value held by the American public, as documented by several public opinion surveys over the past 6 years.

About one-half of the American public believes that computers are a threat to society, and that adequate safeguards do not exist to protect information about people. There is increasing public support for additional government action to protect privacy.

This finding is based on a comprehensive review of public opinion surveys that covered issues of technology and civil liberties, with special attention to the question of privacy and information practices.[48] Most studies, although privately sponsored, were designed and conducted by major public opinion research organizations such as Louis Harris & Associates, the Gallup Organization, the Roper Organization, the National Opinion Research Center, and the major news organizations.

A major difficulty in interpreting existing survey research is that most questions have emphasized general concerns about privacy and civil liberties, rather than specific concerns about the implications of particular uses of computing and information technologies, such as computer matching or computer profiling. As a result, much is known about abstract concerns for privacy, but little about levels of support or opposition to emerging technologies and their use by government agencies. An additional problem of survey research is that the meaning of responses is clouded by definitional differences in what constitutes an invasion of privacy, including definitions ranging from personal freedoms, solitude, and freedom from gossipy neighbors to freedom from governmental or employer surveillance. With these caveats in mind, a number of conclusions and trends about public opinion can be made.

General concern over personal privacy has increased among Americans over the last decade. When asked directly whether they are concerned about threats to personal privacy, most Americans will answer in the affirmative. In several Harris surveys[49] the following question was posed:

---

[46] A total of 142 agencies were surveyed; 5 did not respond at all, and 10 others responded that the question was not applicable or the information was not available, for a net total response of 127 agencies.

[47] Again, 142 agencies were surveyed; a total of 85 computerized law enforcement, investigative, or intelligence record systems were identified. Agencies responded as follows: record quality statistics maintained (3 systems); no record quality statistics (63 systems); no response (17 systems); not applicable or information not available (1 system); and classified (1 system).

[48] William H. Dutton and Robert G. Meadow, "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties and the Democratic Process," OTA contractor report, January 1985.

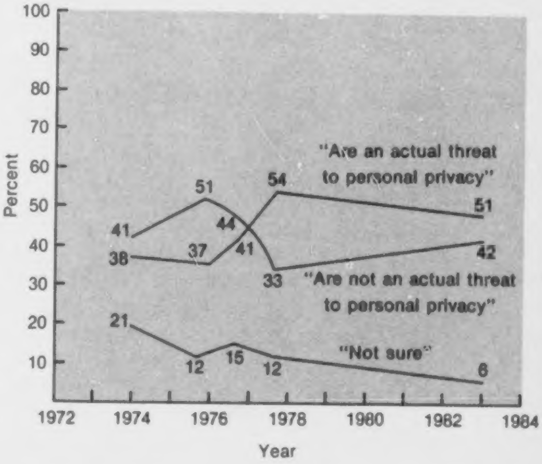
[49] Louis Harris & Associates, Inc., and Dr. Alan F. Westin, *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (conducted for Sentry Insurance), December 1979; and Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its*

> Now let me ask you about technology and privacy. How concerned are you about threats to your personal privacy in America today? Would you say you are very concerned, somewhat concerned, only a little concerned, or not concerned at all?

In 1983, 48 percent of the public described themselves as "very concerned." This was double the 25 percent reported in January 1978 and a marked increase from 31 percent in December 1978. In 1983, an additional 29 percent described themselves as "somewhat concerned," and only 7 percent said they were "not concerned at all," a significant change from the 28 percent who so described themselves in January 1978. In addition, Americans overwhelmingly disagree (64 percent, compared with 27 percent who agree) with the statement that: "Most people who complain about their privacy are engaged in immoral or illegal conduct." In other words, privacy is not merely an instrument for avoiding punishment or detection—it is seen as a legitimate value itself.

Most recently, about one-half of the American public believed that computers were a threat to privacy. As figure 1 indicates, the percentage perceiving computers as a threat has increased since 1974. In 1974, 38 percent of the respondents said computers were a threat and 41 percent said they were not. In 1977, 41 percent said computers were a threat and 44 percent said they were not a threat. In December 1978, 54 percent said they were a threat and only 33 percent indicated they were not. However in 1983, the percentage perceiving computers as a threat to privacy decreased slightly, while the percentage believing that computers are not a threat increased by approximately 10 percent. In 1982, Roper reported that 44 percent were very concerned with reports of abuse of personal information that is stored in computers, and 39 percent were very concerned about "reports of embezzlements and rip-offs through the use of a computer."

Figure 1.—Beliefs That Computers are an Actual Threat to Personal Privacy in This Country[a]



[a] Response to: "Do you feel that the present use of computers are an actual threat to personal privacy in this country, or not?"

SOURCE: Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

An increasing percentage of the public does not believe that the privacy of personal information in computers is adequately safeguarded —from 52 percent in 1978 to 60 percent in 1983. Although a majority of the public (60 percent) believes that computers have improved the quality of life,[50] a larger and increasing (68 percent in 1983) percentage of the public believes that the use of computers must be sharply restricted in the future if privacy is to be preserved.[51]

In general, citizens are concerned with the protections organizations provide for personal information. In 1979, 41 percent agreed and 41 percent disagreed with the statement: "Most organizations that use information about people have enough checks and safeguards against the misuse of personal information." Government agencies were perceived as intrusive by about one-third of the public, with the Central Intelligence Agency, the Federal Bureau of Investigation, and government welfare agencies

---

Leaders on the New Technology and Its Consequences for American Life (conducted for the Southern New England Telephone for presentation at The Eighth International Smithsonian Symposium, December 1983.)

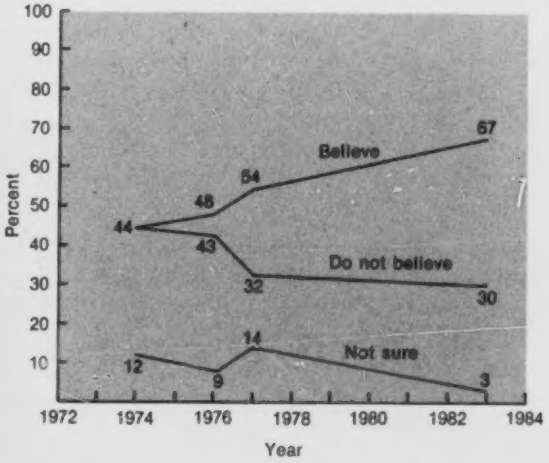
[50] Harris, op. cit., 1979, table 9.2.

[51] Harris, op. cit., 1983, table 3-3.

being mentioned most often as asking for too much personal information. About one-third of the public believe that government agencies should be doing more to maintain the confidentiality of personal information.[52] Most Americans believe that personal information about them is being kept in "some files somewhere for purposes not known" to them. As figure 2 indicates, the percentage of the public believing this to be the case has increased over time, with a high of 67 percent in 1983.

Most Americans, from two-thirds to three-fourths, believe that agencies that release the information they gather to other agencies or individuals are seriously invading personal privacy[53] (see table 4). But, as figure 3 indicates, significant percentages of the public believe that public and private organizations do share information about individuals with others.

Figure 2.—Change in Percent of Public Believing That Files Are Kept on Themselves[a]



[a] Response to: "Do you believe that personal information about yourself is being kept in some files somewhere for purposes not known to you, or don't you believe this is so?"

SOURCE: Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

The American public does not look favorably upon central files and databanks. Most Americans, 84 percent, believe that master files containing personal information, such as credit and employment histories, organizational affiliations, medical history, voting record, phone calls, buying habits, and travel, could be compiled "fairly easily." Only 1 percent of the Harris respondents expressed uncertainty over this possibility. Seventy-eight percent believed that if such a master file were put together, it would violate their privacy.[54]

There is increasing support for additional government action to protect privacy. In 1978, the public was not sure who should be responsible for maintaining privacy. Nearly one-half (49 percent) said it should rest with the people themselves, while 30 percent said the courts, 26 percent Congress, 25 percent the States, 14 percent the President, and 12 percent said employers.[55] Despite confusion over the source of responsibility, two-thirds of the public responded that laws could go a long way to help preserve our privacy.[56] Sixty-two percent of the public thought it was very important that there be an independent agency to handle complaints about violations of personal privacy by organizations.[57] However, 46 percent were opposed to the creation of a National Privacy Protection Agency to protect privacy.[58]

In surveys conducted by the Roper Center in 1982,[59] large majorities believed that laws were needed to govern how information on individuals can be used by organizations that have computer files, and supported the major principles of the "Code of Fair Information Practices." In 1982, 85 percent wanted laws to ensure that corrections of information were included in files, 82 percent said that individ-

---

[52] Harris, op. cit., 1979, tables 2.2, 2.5, 2.6, 2.8, 2.9, 8.1.

[53] Harris, op. cit., 1983, table 1-6.

[54] Ibid., table 1-2.

[55] Harris, op. cit., 1979, table 10.11.

[56] Ibid., table 10.3.

[57] Ibid., table 10.5.

[58] Ibid., table 10.4.

[59] The Roper Center, Institute of Social Research, University of Michigan, contains surveys by the major private polling organizations, including Gallup, Harris, Yankelovich, CBS/New York Times, and Roper. OTA commissioned a keyword search at the Roper Center to locate all previous public opinion research studies on any aspect of attitudes toward government information technology.

Table 4.—Seriousness of Breaches of Confidentiality

Q.: I'm going to read a few things which might be considered an invasion of privacy, all of which deal with computerized information. Do you feel that (READ EACH ITEM) would be a serious invasion of privacy, or not?

		Leaders			
	Total public	Congressmen and top aides	Corporate executives	Media: science editors	Superintendents of schools
Base	1,256	100	100	100	100
The Internal Revenue Service not keeping individual Federal tax returns confidential:					
Serious	84%	98%	93%	95%	89%
Not serious	15	2	7	5	11
The FBI not keeping information about individuals confidential:					
Serious	82	95	93	91	86
Not serious	15	4	6	8	14
Banks sharing information about an individual's banking habits and size of bank accounts:					
Serious	78	66	60	66	78
Not serious	20	30	38	33	22
A credit business selling information about an individual's credit standing:					
Serious	77	64	46	73	75
Not serious	22	34	54	25	25
The Census Bureau not keeping information about individuals confidential:					
Serious	73	88	73	82	75
Not serious	25	11	27	18	25
Insurance companies sharing information gathered about an individual:					
Serious	72	64	63	66	72
Not serious	26	31	35	32	28

SOURCE: Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

uals should be notified of the existence and contents of files containing information about them, 82 percent thought there should be laws to permit people to get copies of any information in files on themselves, and 71 percent thought there should be laws prohibiting most private parties from asking for social security numbers.[60] In addition, 72 percent said businesses should have the right to get information only from the person directly, while only 14 percent said databanks were appropriate.[61]

In the 1983 Harris survey (see table 5), strong majorities of the public and majorities of all four leadership groups supported the enactment of new Federal laws to deal with information abuse, including laws that would require that any information from a computer that might be damaging to people or organizations must be double-checked thoroughly before being used, and laws that would regulate what kind of information about an individual could be combined with other information about the same individual. The authors of the Harris analysis observed that:

> Particularly striking is the pervasiveness of support for tough new ground rules governing computers and other information technology. Americans are not willing to endure abuse or misuse of information, and they overwhelmingly support action to do something about it. This support permeates all subgroups in society and represents a mandate for initiatives in public policy.[62]

Finding 4

The Courts have not developed clear and consistent constitutional principles of information privacy, but have recognized some legitimate

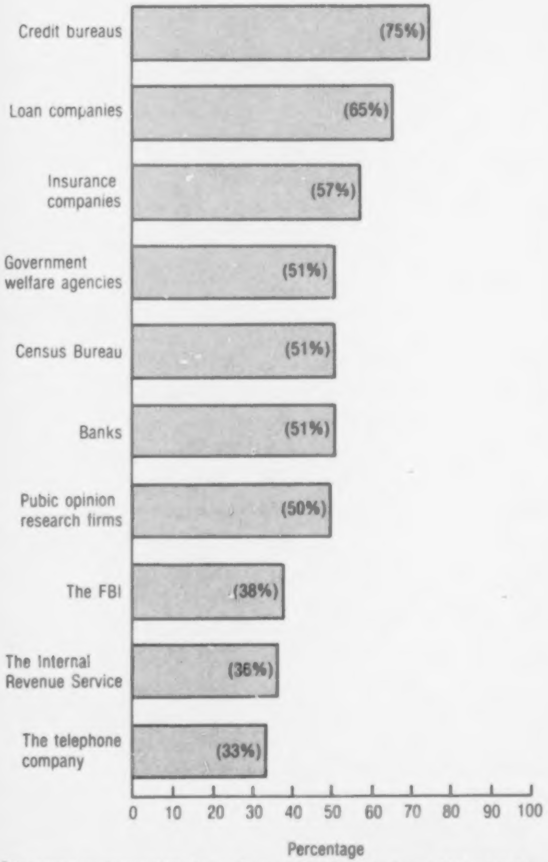
---

[60] Roper 82.6, June 5-12, 1982.

[61] Roper 82.8, August 14-21, 1982.

[62] Harris, op. cit., 1983, p. 41.

Figure 3.—Percent of Public That Believes Each Agency "Shares" Information About Individuals With Others[a]



[a]Response to: "Now I'd like to read you a list of organizations which might have a lot of information about individuals. For each, tell me if you think they do have a lot of information but treat it as strictly confidential, have information and probably share it with others, or don't really have information that people ought to be concerned about whether they share it or not."

SOURCE: Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

expectations of privacy in personal communications.

Although a "right to privacy" is not mentioned in the Bill of Rights, the Supreme Court has protected various privacy interests. The Court has found sources for a right of privacy in the first, third, fourth, fifth, and ninth amendments. Since the late 1950s, the Supreme Court has upheld a series of privacy interests under the first amendment and due process clause, for example, "associational privacy,"[63] "political privacy,"[64] and the "right to anonymity in public expression."[65] The fourth amendment protection against "unreasonable searches and seizures" also has a privacy component. In *Katz v. United States,* the Court recognized the privacy interests that protected an individual against electronic surveillance. But the Court cautioned that:

> . . . the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy from other forms of governmental invasion.[66]

The fifth amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance or compulsory disclosure.[67]

Until *Griswold v. Connecticut,* 381 U.S. 479 (1965), any protection of privacy was simply viewed as essential to the protection of other more well-established rights. In *Griswold,* the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives as an infringement on marital privacy. Justice Douglas, in writing the majority opinion, viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," i.e., the first, third, fourth, fifth and ninth amendments, each of which creates "zones" or "penumbras" of privacy. The majority supported the notion of an independent right of privacy inhering in the marriage relationship. Not all agreed with Justice Douglas as to its source; Justices Goldberg, Warren, and Brennan preferred to lodge the right under the ninth amendment.

---

[63] *NAACP v. Alabama,* 357 U.S. 449 (1958).

[64] *Watkins v. United States,* 354 U.S. 178 (1957), and *Sweezy v. New Hampshire,* 354 U.S. 234 (1957).

[65] *Talley v. California,* 362 U.S. 60 (1960).

[66] *Katz v. United States,* 389 U.S. 347, 350 (1967).

[67] See *Escobedo v. Illinois,* 378 U.S. 478 (1964), *Miranda v. Arizona,* 384 U.S. 436 (1966); and *Schmerber v. California,* 384 U.S. 757 (1966).

Table 5.—Support for Potential Federal Laws on Information Abuse[a]

		Leaders			
	Total public	Congressmen and top aides	Corporate executives	Media: science editors	Superintendents of schools
Base	1,256	100	100	100	100
A Federal law that would require that any information from a computer that might be damaging to people or organizations must be double-checked thoroughly before being used:					
Favor	92%	85%	72%	94%	94%
Oppose	7	12	26	5	5
Federal laws that would make it a criminal offense if the privacy of an individual were violated by an information-collecting business or organization:					
Favor	83	80	79	94	88
Oppose	14	10	17	5	12
A Federal law that would call for the impeachment of any public official who used confidential information to violate the privacy or take away the freedom of an individual or a group of individuals without a proper court order or a court trial:					
Favor	81	69	89	85	91
Oppose	17	26	10	15	8
Federal laws that would require punishment for those in authority responsible for computer mistakes, such as mistakes that hurt people's credit ratings, harm companies, or endanger lives:					
Favor	71	53	37	69	61
Oppose	25	41	61	25	37
Federal laws that could put companies out of business which collected information about individuals and then shared that information in a way that violated the privacy of the individual:					
Favor	68	65	78	78	77
Oppose	30	27	20	20	21
Federal regulations on just what kind of information about an individual could be combined with other information about the same individual:					
Favor	66	77	65	81	87
Oppose	28	18	31	16	13

[a]Response to: Would you favor or oppose (READ EACH ITEM)?

SOURCE: Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

In *Eisenstadt v. Baird*, 405 U.S. 438 (1972),[68] the Court extended the right to privacy beyond the marriage relationship to lodge in the individual:

> If the right of the individual means anything, it is the right of the *individual*, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.

Roe v. Wade, 410 U.S. 113 (1973),[69] further extended the right of privacy "to encompass a woman's decision whether or not to terminate her pregnancy." The Court argued that the right of privacy was "founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action." The District Court had argued that the source of the right was the ninth amendment's reservation of right to the people.

---

[68] In which the Court struck down a Massachusetts law that made it a felony to prescribe or distribute contraceptives to single persons.

[69] In which the Court struck down the Texas abortion statute.

In the earliest case that raised the issue of the legitimate uses of computerized personal information systems, the Court avoided the central question of whether the Army's maintenance of such a system for domestic surveillance purposes "chilled" the first amendment rights of those whose names were contained in the system.[70] In two cases decided in 1976, the Court did not recognize either a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters[71] or one that protected the individual's interests with respect to bank records.[72] In *Paul v. Davis,* the Court specified areas of personal privacy considered "fundamental":

> . . . matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.[73]

Davis' claim of constitutional protection against disclosure of his arrest on a shoplifting charge was "far afield from this line of decisions" and "we decline to enlarge them in this manner."[74] In *United States v. Miller,* the Court rejected Miller's claim that he had a fourth amendment reasonable expectation of privacy in the records kept by banks "because they are merely copies of personal records that were made available to the banks for a limited purpose," and ruled instead that "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[75]

In *Whalen v. Roe,* the Court for the first time recognized a right of information privacy, noting that the constitutionally protected "zone of privacy" involved two kinds of interests—"One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[76] In this case, a unanimous Court upheld a New York law requiring the State to maintain computerized records of prescriptions for certain drugs, because "the New York program does not, on its face, pose a sufficiently grievous threat to either interest to establish a constitutional violation."[77] The Court held that as long as the security of a computer is adequate and the information is only passed to appropriate officials, sensitive information may be stored and retrieved without an invasion of a person's right to privacy. In another case in 1977,[78] the Court used a test similar to the one developed in *Whalen*, i.e., balancing the extent of the privacy intrusion against the interests that the intrusion advanced, holding that:

> In sum, appellant has a legitimate expectation of privacy in his personal communications. But the constitutionality of the Act must be viewed in the context of the limited intrusion of the screening process, of appellant's status as a public figure, of this lack of any expectation of privacy in the overwhelming majority of the materials, of the important public interest in preservation of the materials, and of the virtual impossibility of segregating the small quantity of private materials without comprehensive screening.[79]

The court did reaffirm that one element of privacy is "the individual interest in avoiding disclosure of personal matters."[80]

In subsequent lower court cases involving the question of information privacy, the circuit courts have not uniformly followed *Whalen v. Roe.*[81] For example, the Seventh and Ninth Circuit Courts have used autonomy interests rather than informational privacy interests as the basis for their rulings.[82] In *McElrath v. Califano,* the Seventh Circuit Court reiterated that the constitutional right to privacy extends only to those personal rights deemed "fundamental" or "implicit in the concept of ordered liberty," and that "the claim of the appellants to receive welfare benefits on their own informational terms does not rise to the level of a constitutional guarantee."[83] In *St. Michael's Convalescent Hospital v. California,* the Ninth Circuit Court ruled that:

---

[70] *Laird v. Tatum* 408 U.S. 1 (1972).

[71] *Paul v. Davis* 424 U.S. 693 (1976).

[72] *United States v. Miller* 425 U.S. 435 (1976).

[73] *Paul v. Davis,* 424 U.S. 693, 713 (1976).

[74] Id. at 713.

[75] *U.S. v. Miller,* 425 U.S. 435, 442 (1976). In response to this decision, Congress passed the Right to Financial Privacy Act of 1978 (Public Law 95-630) providing bank customers with some privacy regarding records held by banks and other financial institutions and providing procedures whereby Federal agencies can gain access to such procedures.

[76] *Whalen v. Roe* 429 U.S. 589, 599-600 (1977).

[77] Id. at 600.

[78] *Nixon v. Administrator of General Services,* 433 U.S. 425, in which the Court upheld a Federal law that required the national archivists to examine written and recorded information accumulated by the President. Nixon challenged the act's constitutionality on the grounds that it violated his right of privacy.

[79] Id. at 465.

[80] Id. at 457.

[81] See Gary R. Clouse, "The Constitutional Right to Withhold Private Information," *Northwestern University Law Review,* vol. 77, 1982, p. 536.

> As in *Paul v. Davis,* their [appellants] claim is not based upon any contention that the public disclosure of the cost information will "restrict [their] freedom of action in a sphere contended to be private." We conclude that no cognizable constitutional right of privacy is implicated here.[84]

In 1980, the Third Circuit used *Whalen* to uphold the National Institute for Occupational Safety and Health's request that an employer produce certain medical records of its employees.[85] The Court ruled that:

> The privacy interest asserted in this case falls within the first category referred to in *Whalen v. Roe,* the right not to have an individual's private affairs made public by the government. There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.[86]

In a 1981 case involving the compilation and disclosure of juveniles' social histories, the Sixth Circuit explicitly addressed the question of the relationship between *Paul v. Davis* and *Whalen v. Roe,* stating that:

> We do not view the discussion of confidentiality in *Whalen v. Roe* as overruling *Paul v. Davis* and creating a constitutional right to have all government action weighed against the resulting breach of confidentiality. The Supreme Court's discussion makes reference to only two opinions—*Griswold v. Connecticut, supra* in which the court found that several of the amendments have a privacy penumbra, and *Stanley v. Georgia, supra,* a first amendment case—neither of which support the proposition that there is a general right to nondisclosure.[87]

The Sixth Circuit Court went on to state that:

> . . . absent a clear indication from the Supreme Court we will not construe isolated statements in *Whalen* and *Nixon* more broadly than their context allows to recognize a general constitutional right to have disclosure of private information measured against the need for disclosure.[88]

The Supreme Court has not yet accepted a case to clarify the meaning and breadth of *Whalen.*

---

[82] See: *McElrath v. Califano,* 615 F.2d 434 (7th Cir. 1980) which upheld Federal and State regulations that require all family members to disclose their social security numbers as a condition for receiving Aid to Families With Dependent Children benefits; and *St. Michael's Convalescent Hospital v. California,* 643 F.2d 1369 (9th Cir. 1981) which upheld a California statute requiring that all health care providers who are reimbursed through the Medi-Cal program release their cost information to the public.

[83] *McElrath v. Califano,* 615 F.2d 434,441 (7th Cir. 1980).

[84] *St. Michael's Convalescent Hospital v. California,* 643 F.2d 1369, 1375 (9th Cir. 1981).

[85] *United States v. Westinghouse,* 638 F.2d 570 (3d Cir. 1980).

[86] Id. at 577.

[87] *J.P. v. DeSanti,* 653 F.2d 1080, 1089 (6th Cir. 1981).

[88] Id.

Chapter 3

Computer Matching To Detect Fraud, Waste, and Abuse

Contents

Page
Summary 37

Introduction 38

Background 40
  Technology 40
  Policy History 41

Findings 43
  Finding 1 43
  Finding 2 46
  Finding 3 50
  Finding 4 52
  Finding 5 53
  Finding 6 55
  Finding 7 57
  Finding 8 58
  Finding 9 59
  Finding 10 61
  Finding 11 62

Tables

Table No. *Page*
6. Project Match Information Disclosures 42
7. Statutes Authorizing Specific Computer Matches 46
8. Computer Matches Reported to the PCIE Long-Term Computer Matching Project 48
9. Computer Matching Programs Reported to OTA 49
10. Examples of Cost/Budget Analyses 52
11. Costs and Benefits of Wage Matching 52
12. Estimated Costs and Benefits of Computer Matching in Four Sites 52

Figure

Figure No. *Page*
4. Computer Matches Conducted From April 1980 to April 1985 49

Chapter 3

Computer Matching To Detect Fraud, Waste, and Abuse

SUMMARY

Computer matching involves the comparison of two or more sets or systems of computerized records to search for individuals who may be included in more than one file. Matching can be done manually with paper files. But, as a practical matter, time and cost requirements make manual matching prohibitive in cases involving a large number of records. The primary impetus for Federal and State use of computer matching is to detect fraud, waste, and abuse in government welfare and social service programs. However, computer matching has broad applicability to government programs and activities.

Computer matching has the potential to improve the efficiency of government recordkeeping and management of government programs. It is widely used by many States and foreign countries, the private sector, and increasingly by the Federal Government, where the technique is strongly supported by the Office of Management and Budget (OMB) and the inspectors general, among others, and has been endorsed in several public laws.

However, a number of problems have been identified in Federal computer matching activities, including weak oversight, little persuasive evidence or documentation of cost-effectiveness, widely variable record quality, and little consideration of the implications for privacy and civil liberties.

In computer matching, the basic policy conflict is between the efficient management of government programs (including effective law enforcement) and the rights of individuals. The fourth amendment protects "persons, houses, papers, and effects" against unreasonable government searches and seizures. The Privacy Act of 1974 requires that information collected for one purpose not be used for another purpose, unless, among other exemptions, it falls within a "routine use." Under OMB guidelines, personal information used in computer matches can be disclosed under the routine use exemption.

OTA's assessment of computer matching technology and policy issues found that:

- Although Congress has legislated general and specific restrictions on agency disclosure of personal information, it has also endorsed computer matching and other record linkages in various programmatic areas specified in several public laws. Thus, congressional actions appear to be contradictory.
- It is difficult to determine how much computer matching is being done by Federal agencies, for what purposes, and with what results. However, OTA estimates that in the 5 years from 1980 to 1984, the number of computer matches nearly tripled.
- As yet, no firm evidence is available to determine the costs and benefits of computer matching and to document claims made by OMB, the inspectors general, and others that computer matching is cost-effective.
- The effectiveness of computer matches used to detect fraud, waste, and abuse can be compromised by inaccurate data.
- There are numerous procedural guidelines for computer matching, but little or no oversight, follow-up, or explicit consideration of privacy implications.
- As presently conducted, computer matching programs may raise several constitutional questions, e.g., whether they violate protection against unreasonable search and seizure, due process, and equal pro-

tection of the laws. But, as presently interpreted by the courts, the constitutional provisions provide few, if any, protections for individuals who are the subjects of matching programs.

- The Privacy Act as presently interpreted by the courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.
- The courts have been used infrequently as a forum for resolving individual grievances over computer matching, although some organizations have brought lawsuits.
- Computer matches are commonly conducted in most States that have the computer capability. At least four-fifths of the States are known to conduct computer matches, most in response to Federal directives.
- All Western European countries and Canada are using computer matching or record linkages, to an increasing degree, as a technique for detecting fraud, waste, and abuse.
- In designing policy for computer matching, consideration of the following factors is important:
  - —which records to make available for computer matches and for what purposes,
  - —approval required before a match takes place,
  - —notice to individuals,
  - —whether to require a cost-benefit analysis,
  - —verification of hits, and
  - —appropriate action to be taken against an individual who has submitted false information.

In response to the OTA survey of Federal agencies, OTA determined that:

- Forty-three percent of agency components that reported participation in computer matching activities (16 out of 37) said that the matches were required or authorized by legislation.
- Eleven cabinet-level departments and four independent agencies carried out a total of 110 matching programs, with a total of 553 matches conducted from 1980 to April 1985.
- In the 5 years from 1980 to 1984, the number of computer matches nearly tripled.
- For 20 percent of the matches reported, information was available on the number of records matched, number of hits, and percent of hits verified.
- Despite the low percentage of respondents providing information on reported matches, the number of separate records used in the reported matching programs totaled over 2 billion; the total number of records matched was reported to be over 7 billion due to multiple matches of the same records.
- The percentage of hits (i.e., matches between the specific items of interest in two different records) verified to be accurate ranged from 0.1 to 100 percent.
- Sixty-eight percent (25 of 37) of the agencies indicating that they participated in matching programs said that procedures were used to ensure that the subject record files contain accurate information.

INTRODUCTION

Computer matching involves the electronic comparison of two or more sets or systems of personal records.[1] Matching is used to check for individuals who should not appear in two systems of records, as in the case of Federal employees above a certain salary level and persons receiving food stamps. Matching can also be used to locate individuals who should appear in two systems of records but do not; for example, males registered for the draft and males over the age of 18 with driver's licenses. Although manually comparing the contents of two record systems is a traditional audit technique, this practice becomes prohibitive when dealing with massive record systems that are not uniformly comparable with other record systems. Computers greatly facilitate such comparisons.

---

[1] The Office of Management and Budget (OMB) Guidelines, issued May 11, 1982, define computer matching as "a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set."

Because of the number of people who may be subject to computer matching and because it can be done without their knowledge, computer matching has raised a number of policy questions. The basic conflict is between the efficient management of government programs and the rights of individuals.

It is well known that government programs are subject to fraud, waste, and abuse. Although the problem is not peculiar to welfare programs, fraud and waste in these programs have been particularly well documented. For example, the General Accounting Office (GAO) reviewed improper payments for fiscal year 1978-79 in 5 of the 58 federally supported welfare programs, and estimated that Federal and State welfare agencies spent about $867 million on erroneous welfare payments because recipients had not properly reported their income and assets.[2]

Since 1977, computer matching has been used extensively by a number of Federal departments and State agencies. Some specific examples of matching include:

1. recipients of Aid to Families With Dependent Children (AFDC) matched with the Social Security Administration's earnings record,
2. the Veterans Administration's rolls matched with the supplemental security income (SSI) benefit rolls,
3. AFDC recipients matched with Federal civilian and military payrolls, and
4. State AFDC rolls matched with other State AFDC rolls.

In general, matching is used to detect unreported income, unreported assets, duplicate benefits, incorrect social security numbers, overpayments, ineligible recipients, incongruous entitlements (SSI checks mailed to deceased individuals, mothers claiming more children than exist), present addresses of individuals (Parent Locator Service, Student Loan defaulters), and providers billing twice for the same service.

In order to facilitate computer matching, a number of computerized databanks have been created solely for matching purposes. One example is the Medicaid Management Information System that contains information on recipient records, provider data, and claims-processing information.[3] A proposed computerized databank is the Internal Revenue Service (IRS) Debtor Master File that will contain the names of all delinquent Federal borrowers to match against tax returns.[4]

A central policy issue is whether and under what conditions the use of computer matching is appropriate, given the rights of individuals who are the subjects of matching and given the possible long-term societal effects of general electronic searches, as elaborated below.

As discussed in chapter 2, public opinion polls indicate that Americans value their privacy and generally expect that activities in one area of their lives are kept separate from those in other areas. In the 1983 Harris Survey, most Americans (from two-thirds to three-fourths) responded that agencies that release the information they gather to other agencies or individuals are seriously invading personal privacy.[5] Two-thirds or more of Americans surveyed believed that the following government information practices would entail a "serious invasion of privacy"—the IRS not keeping individual tax records confidential (84 percent perceived this as a serious invasion); the Federal Bureau of Investigation not keeping information about individuals confidential (82 percent viewed as serious invasion); and the Census Bureau not keeping information about individuals confidential (73 percent viewed as serious invasion). Yet, in a 1979 survey, 87 percent of respondents believed that government agencies were justified in using computers to check welfare rolls against employment records to identify people claiming benefits to which they are not entitled. However, they were less supportive (68 percent) of the IRS use of matching to check tax returns against credit card records.[6]

---

[2] U.S. General Accounting Office, "Legislative and Administrative Changes To Improve Verification of Welfare Recipients' Income and Assets Could Save Hundreds of Millions," HRD-82-9, Jan. 14, 1982.

[3] U.S. Department of Health and Human Services, Health Care Financing Administration, "Medicare and Medicaid Data Book," 1982.

[4] Judith A. Sullivan, "IRS To Create Debtor File," *Government Computer News*, Nov. 8, 1985, pp. 1, 70.

[5] Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life*, (conducted for Southern New England Telephone for presentation at The Eighth International Smithsonian Symposium, December 1983), table 1-6.

Public opinion polling results suggest that Americans recognize that a balance must be struck between individual rights and the protection of society. A majority of the public believes that there are some costs in terms of privacy that must be paid in order to have a more lawful society. In response to the statement: "In order to have effective law enforcement, everyone should be prepared to accept some intrusion into their personal lives," 57 percent agreed and 36 percent disagreed.[7] Public opinion research also indicates that Americans have certain expectations about the scale of government monitoring activities. Americans assume that government investigations are predicated on evidence of individual wrongdoing and that procedural standards and safeguards exist for investigative behavior. The public overwhelmingly believes the police should not be able to tap the telephones of members of suspicious organizations without obtaining a court order. A large majority of the public is concerned about protecting records from examination by public authorities without a court order. Over 80 percent of the public believes that the police should not be able to examine the bank records of suspicious individuals without a court order.[8]

Computer matches can also conflict with the expectation of being treated as an individual. Computer matches are inherently mass or class investigations, as they are conducted on a category of people rather than on specific individuals. In theory, no one is free from these computer searches; in practice, welfare recipients and Federal employees are most often the targets.

---

[6] Louis Harris & Associates, Inc., and Alan F. Westin, *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (conducted for Sentry Insurance, 1979), table 9.3.

[7] Ibid., table 2.2.

[8] Ibid., table 8.3.

BACKGROUND

Technology

In conducting a computer match, one computer file is compared with another using software that instructs the computer to search for certain patterns, e.g., duplicate social security numbers, same names, identical addresses. Before a match is conducted, agency personnel need to determine whether the relevant data are formatted in a similar fashion on the two or more systems being matched. If not, then the data need to be reformatted or the software must be designed to take the differences into account.

Files can be compared either by using computer tapes of the record systems or by direct electronic linkages of computers. At the present time, the matching of tapes is the procedure commonly used. However, as systems become more compatible and costs drop, direct electronic linkages between/among systems are likely to increase.

During the match, computer files are compared on the basis of a specified data element as an identifier, generally the social security number. Experience from early computer matches suggested that social security numbers were often inaccurate. In order to ensure the effectiveness of a computer match, a search for erroneous social security numbers can be conducted before the match. Additionally, the identifier used for the match can be the social security number plus another data element, such as the first few letters of a last name.

The social security number is not essential to computer matches as databases can also be searched for combinations of selected factors; however, a unique identifier makes matching far easier. In 1981, congressional legislation required that every member of a household receiving food stamps must have a social security number. Such a requirement makes matching more efficient because it is easier to identify duplicate or fraudulent recipients.

The resulting match produces information on individuals who are common to the two files; for example, an individual who has not repaid a Federal student loan may also be a Federal employee, or a physician may have billed Medicaid twice for the same service. Once the match has identified the files having duplicate or similar information, these files are considered "hits." The hits must then be verified manually to determine whether the same individual is really involved and whether there is cause to believe that the individual has committed fraud.

Policy History

In the early 1970s, a few States began to use computer matching to check AFDC recipients against wage information from the State Employment Security agencies. The first major computer match at the Federal level was Project Match, announced in November 1977 by Joseph Califano, Secretary of the Department of Health, Education, and Welfare (HEW). Project Match compared computer tapes of welfare rolls and Federal payroll files in 18 States, New York City, the District of Columbia, and parts of Virginia. The goal was to detect government employees who were fraudulently receiving AFDC benefits. Privacy advocates in Congress, members of the Privacy Protection Study Commission, the American Civil Liberties Union, and others criticized the proposed match as a "fishing expedition."

There were disputes within the general counsel's office at HEW regarding the legal implications of conducting these matches, especially in light of the Privacy Act's "routine use" provisions.[9] There were also disputes between HEW and the Civil Service Commission (CSC) and the Department of Defense (DOD), neither of which wanted to release its tapes because of the routine use provision.[10] The general counsel at CSC raised two concerns regarding the compatibility of the proposed match with the routine use provision of the Privacy Act: first, "it is evident that this information on employees was not collected with a view toward detecting welfare abuses," and second, "that disclosure of information about a particular individual at this preliminary stage is (not) justified by any degree of probability that a violation or potential violation of law has occurred."[11] CSC and DOD eventually released their tapes to HEW—CSC justifying the transfer on the argument that HEW could get the information under the Freedom of Information Act if it so chose, and DOD justifying the transfer as a new "routine use" under the Privacy Act. HEW lawyers, themselves, were additionally concerned that the results of the match would need to be transferred to the employing departments for verification, which would also raise Privacy Act issues. As table 6 indicates, it was possible to justify under existing law all record transfers required by Project Match.

While Project Match was under way, an interagency advisory group of Federal personnel officials questioned whether Federal employees should be notified under the Privacy

---

[9] See Jake Kirchner, "Privacy—A History of Computer Matching in the Federal Government," *Computerworld*, Dec. 14, 1981, pp. 1-16. Section 3b of the Privacy Act establishes the conditions under which an agency can disclose personal information to another party without the prior consent of the individual. One of these conditions of disclosure is "for a routine use," defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" [3(a)(7)]. All routine uses are to be published in the *Federal Register*, including "the categories of users and the purpose of such use" [3(e)(4)(D)].

[10] For correspondence, see Kirchner, op. cit., and pp. 122-125 of U.S. Congress, Senate, Hearings Before the Senate Subcommittee on Oversight of Government Management, Committee on Governmental Affairs, *Oversight of Computer Matching To Detect Fraud and Mismanagement in Government Programs* (Washington DC: U.S. Government Printing Office, Dec. 15-16, 1982) [hereafter referred to as the Cohen hearings].

[11] See Cohen hearings, op. cit., p. 123.

Table 6.—Project Match Information Disclosures

Disclosure	Justification
Health, Education, and Welfare Department disclosure of social security number and birth dates to other agencies	Exception in Privacy Act
Office of Personnel Management disclosure to Health, Education, and Welfare Department	Public interest outweighs personal privacy outlined in the Privacy Act and information could be obtained under the Freedom of Information Act
Defense Department disclosure of military personnel on active duty to Health, Education, and Welfare Department	Exception under "routine use" of the Privacy Act
State government disclosure of State Aid to Families With Dependent Children (AFDC) rolls to Health, Education, and Welfare Department	Privacy Act does not apply to States; no Federal law barring such disclosure
State government disclosure of State AFDC rolls to Federal employer agencies	New "routine use" published in the Federal Register based on original routine uses
Agencies disclosure of annotated work sheets to the Health, Education, and Welfare Department	HEW Inspector General Statute requiring agencies to respond to information requests by Inspector General
Agencies disclosure of civil or criminal proceedings to Health, Education, and Welfare Department	Exception in Privacy Act
Health, Education, and Welfare Department disclosure to State or local agencies	Exception in "routine use" of Privacy Act to assist States and localities enforce violated statutes
Agencies refer information and case to Department of Justice when lawbreaking is suspected	Exception under "routine use" or law enforcement exception of the Privacy Act
Agencies referral of cases to other agencies when lawbreaking is suspected or for investigation of government employees	For administrative action authorized by the "routine uses" of Privacy Act

SOURCE: Kenneth James Langan, "Computer Matching Programs: A Threat to Privacy?" *Columbia Journal of Law and Social Problems*, vol. 15, No. 2, 1979, pp. 149-150.

Act of the record transfers. The Department of Justice argued against notification, saying, "We view Project Match as a law enforcement program, designed to detect suspected violations of various criminal statutes in (government) operations."[12] Opponents of the match pointed out that such a view was hardly consistent with the "routine use" concept.[13] By March 1978, Project Match had identified 7,100 employees who were possibly ineligible for welfare. But, it had also generated so much information that agency officials could not follow up adequately to determine the validity of that information.[14]

After Project Match was completed, Secretary Califano advocated more Federal use of matching and tried to access private sector company files. This increased public pressure for justification of matching under the Privacy Act, and OMB and the Carter White House began to take a more active role in the process. In late 1977, OMB sent a letter to Representative Richardson Preyer to explain the Administration's justifications for Project Match, concluding that "the requirement of compatible purpose in the routine use is difficult and is ultimately largely a matter of judgment."[15]

While Project Match was being run, the White House was concurrently conducting its Privacy Initiative, following the 1977 report of the Privacy Protection Study Commission. The conflict between the goals of the Privacy Initiative and Project Match was not ignored within the White House, but remained unresolved. In response to concerns about Project Match's privacy implications, OMB took on the task of writing guidelines for computer matching, with input from the President's Office of Telecommunications Policy and the White House Privacy Initiative.

In 1979, Congress required States to conduct wage matching for AFDC recipients. Because computer matching was perceived as an efficient tool for managing benefit programs, States increasingly began to use it for a number of programs and with a number of sources, including private institutions such as employers and banks. One of the largest and best publicized of the State efforts occurred in Massachusetts in 1982 when welfare recipients were matched against bank records, identifying about 600 people who had bank accounts larger than regulations allowed. About 160 of those persons identified received termination notices. But for more than 110 of these 160 persons, the identification based on the computer match was later determined to be based on erroneous information, e.g., inaccurate social security number or bank account for burial expenses held in trust.[16]

---

[12] Kirchner, op. cit., p. 7.

[13] See testimony of John Shattuck of the American Civil Liberties Union, Cohen hearings, op. cit., p. 80.

[14] Laura B. Weiss, "Government Steps Up Use of Computer Matching To Find Fraud in Programs," *Congressional Quarterly Weekly Report*, Feb. 26, 1983, p. 432.

[15] Kirchner, op. cit., p. 10.

Since 1979, concern about the size and efficiency of the Federal Government and the increase in the Federal deficit has made management a policy priority for both Congress and the executive branch. One effect has been to encourage the use of computer matching, especially as a technique to detect fraud, waste, and abuse. In 1981, President Reagan established the President's Council on Integrity and Efficiency (PCIE), chaired by the Deputy Director of OMB, to enhance interagency efforts to reduce fraud and waste, and to give the inspectors general a direct link to the President. PCIE's projects include: 1) a long-term computer matching project; 2) Project Clean Data (i.e., standardization of data elements); and 3) an inventory of State computer matching software packages. President Reagan has also formed the President's Council on Management Improvement, composed of the senior management official from each major department and agency (including central management agencies—OMB, the General Services Administration, and the Office of Personnel Management), the Assistant to the President for Policy Development, and the Assistant to the President for Presidential Personnel. Its purpose is to advise the President and to oversee agency implementation of management reforms.

In 1982, President Reagan established the President's Private Sector Survey on Cost Control, popularly known as the Grace Commission, to study management problems in government. Its major finding was "that the Federal Government has significant deficiencies from managerial and operating perspectives, resulting in hundreds of billions of dollars of needless expenditures . . . "[17] There have been criticisms of the Grace Commission's cost figures and its methodology.[18] In 1982, the Reagan Administration also announced Reform '88, a program to increase efforts to reduce waste, fraud, and abuse, and to restructure the management and administrative systems of the Federal Government.

---

[16] Ross Gelbspan, "Computer Matching Stirs Up Criticism," *Boston Globe*, June 9,1985, p. A1, cont. A4.

[17] Ellen Law, "Grace Reports To the President," *Government Computer News*, March 1984, p. 4.

[18] Steven Kelman, "The Grace Commission: How Much Waste in Government?" *The Public Interest*, No. 78, winter 1985, pp. 62-82.

FINDINGS

Finding 1

Although Congress has legislated general and specific restrictions on agency disclosure of personal information, it has also endorsed computer matching and other record linkages in various programmatic areas specified in several public laws. Thus, congressional actions appear to be contradictory.

As discussed in chapter 2, Congress has passed a number of laws that give an individual certain rights with respect to controlling the use of personal information, and that place restrictions on the ways in which agencies may legitimately use such information. These laws speak both to general agency practices (e.g., the Privacy Act of 1974) and to the practices of specific agencies, (e.g., Section 6103 of the Tax Reform Act of 1976).

Congress has also legislated a number of exchanges of information among agencies. Congressional concern with detecting fraud, waste, and abuse has resulted in several major legislative endeavors that have been viewed as authorizing computer matching. First is the establishment of inspectors general offices in a number of Federal agencies to identify and reduce fraud, waste, and abuse, and to identify and prosecute perpetrators (Public Law 94-452, Public Law 94-505, Public Law 97-252). The Departments of Health and Human Services, Energy, Defense, and 15 other Federal agencies have inspectors general. The inspectors general are potentially very powerful officers who:

> . . . have complicated reporting relationships involving department and agency heads, and Congress and its many committees. IGs can bypass department/agency general counsels and take matters directly to the Criminal Division of the Justice Department. They can initiate audits and investigations at any time, which can cover fraud, abuse, and any and all management deficiencies.[19]

Inspectors general employ a variety of techniques, including: 1) vulnerability assessments to assess the risk of loss in programs, 2) management control guides, 3) fraud bulletins and memos, 4) fraud control training, 5) hotlines for reports of wrongdoing, and 6) audit follow-up procedures. Matching, profiling, and front-end verification are used by inspectors general.

A second legislative endeavor that is perceived as encouraging data-sharing among agencies is the Paperwork Reduction Act of 1980 (Public Law 96-511), which gives OMB Federal information oversight authority and the responsibility to promote the effective use of information technology. It establishes an Office of Information and Regulatory Affairs within OMB to carry out the purposes of the act, oversee agency compliance, and set up a Federal Information Locator System to register all information collection requests. OMB Circular A-130 was issued in December 1985 as an integrative policy statement on information resource management policies, including privacy and matching.[20]

A statute that may encourage the sharing of information within an agency is the Federal Managers Financial Integrity Act of 1982 (Public Law 97-255), which requires periodic evaluations of and reports on agency systems of internal control and action to reduce fraud, waste, abuse, and error. OMB Circular A-123 (October 28, 1981) complements the act by mandating an improvement in internal control systems, including a requirement that agency heads issue specific internal control directives and review plans for all components of their agencies. Inspectors general have the responsibility to review directives. OMB Assistant Director Wright and Comptroller General Bowsher have pledged that:

> OMB and GAO plan to work together very closely in implementing the Act and in assuring that the momentum already built up within the agencies for improved internal control is sustained.[21]

A fourth statute that encourages exchanges of personal information is the Debt Collection Act of 1982 (Public Law 97-365), which establishes a system of data-sharing between Federal agencies and private credit reporting agencies in order to increase the collection of delinquent nontax debts. The act permits agencies to:

1. refer delinquent nontax debts to credit bureaus to affect credit ratings;
2. contract with private firms for collection services;
3. require applicants for Federal loans to supply their taxpayer identification numbers (social security numbers);
4. offset the salaries of Federal employees to satisfy debts owed the government;
5. screen credit applicants against IRS files to check for tax delinquency;

---

[19] John D. Young, "Reflections On the Root Causes of Fraud, Abuse and Waste in Federal Social Programs," *Public Administration Review*, 1983, p. 366.

[20] Office of Management and Budget, "Management of Federal Information Resources," Circular No. A-130, Dec. 12, 1985.

[21] Office of Management and Budget, "Agencies to Tighten Internal Control Systems," OMB 82-26 (President's Task Force on Management Reform), Oct. 8, 1982.

6. turn over to private contractors the mailing addresses of delinquent debtors obtained from IRS;
7. extend from 6 to 10 years the statute of limitations for collection of delinquent debts by administrative offset; and
8. charge interest, penalties, and administrative processing fees on delinquent nontax debts.

The law requires agencies to provide due process to individuals before using any of the newly authorized methods of collection. The law provides safeguards to preserve the confidentiality of taxpayer information, and civil and criminal penalties are included when taxpayer addresses are improperly disclosed. OMB estimates that the improved procedures and newly available tools will result in an additional $500 million in annual collections.[22] OMB has decided that:

> Rather than creating a new bureaucracy to implement the credit reporting provisions of the Debt Collection Act, the existing nationwide network of commercial and consumer credit bureaus will be under contract to provide this service for all departments and agencies.[23]

The statute requiring the most far-reaching data-sharing is the Deficit Reduction Act of 1984 (DEFRA) (Public Law 98-369), which requires the establishment of new State information systems for verification purposes and the use of verification in a number of federally funded State-administered programs. This 1,210-page law provides tax reforms and spending reforms, primarily by amending the Social Security Act and Internal Revenue Code. Provisions that are relevant to management and efficiency are in Subtitle C—"Implementation of Grace Commission Recommendations," Section 2651.

The major changes in the Social Security Act mandated by DEFRA include requiring States or State agencies to: 1) have an income and eligibility system, 2) obligate recipients to supply their social security numbers and require States to use those numbers in the administration of programs, 3) compel employers to keep quarterly wage information, 4) exchange relevant information with other State agencies and with the Department of Health and Human Services, and 5) notify recipients and applicants that information available through the system will be requested and utilized. The programs that must participate in the income verification program are: AFDC; Medicaid; unemployment compensation; food stamps; and any State program under a plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Under DEFRA, no Federal, State, or local agency may terminate, deny, suspend, or reduce any benefits of an individual until such agency has taken appropriate steps to independently verify information.

DEFRA provides certain procedural rights for the individual, including that the agency shall inform the individual of the findings made on the basis of verified information, and give the individual an opportunity to contest such findings. DEFRA makes a number of changes in the Internal Revenue Code, including that the Commissioner of Social Security shall, on request, disclose information on earnings from self-employment, wages, and payments on retirement income to any Federal, State, or local agency administering one of the following programs: AFDC; medical assistance; supplemental security income; unemployment compensation; food stamps; State-administered supplementary payments; and any benefit provided under a State plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Information with respect to unearned income may also be disclosed from the IRS files to the above agencies.

In addition to these broad endorsements of and requirements for computer matches, there are a number of statutes that authorize specific computer matches (see table 7).

Congressional restrictions on agency disclosures of personal information and congres-

---

[22] Office of Management and Budget, "OMB Announces Progress in Administration's Debt Collection Effort," OMB 82-32 (Reform '88 Communications), Dec. 15, 1982.

[23] Office of Management and Budget, "Government to Use Credit Bureaus to Cut Delinquent Debts; Delinquency Growth Halted," OMB 83-29 (Public Affairs/Management), Sept. 23, 1983.

Table 7.—Statutes Authorizing Specific Computer Matches

Tax Reform Act of 1976, Public Law 94-455, permitted the Department of Health, Education, and Welfare to search the databanks of other Federal agencies to locate parents who fail to pay child support.

Social Security Amendments of 1977, Public Law 95-216, required States to use wage data in determining eligibility for Aid to Families With Dependent Children (AFDC) Program benefits by providing them access to earnings information held by the Social Security Administration (SSA) and State employment security agencies.

Food Stamp Act Amendments of 1977, Public Law 96-58, granted access to employer-reported wage information for recipients of supplementary security income (SSI) benefits.

Food Stamp Act Amendments of 1980, Public Law 96-249, amended the Internal Revenue Code and the Social Security Act to allow State food stamp agencies to obtain and use wage, benefit, and other information in SSA files and those of State unemployment compensation agencies.

Food Stamp and Commodity Distribution Amendments of 1981, Public Law 97-98, required States to obtain and use earnings information obtained from employers.

Department of Defense Authorization Act of 1983, Public Law 97-252, required the Secretary of Education to prescribe methods for verifying that individuals receiving any grant, loan, or work assistance under Title IV of the Higher Education Act of 1965 had complied with registration as necessary under the Military Selective Service Act.

Deficit Reduction Act of 1984, Public Law 98-369, required the Internal Revenue Service (IRS) to disclose information about an individual's unearned income to State welfare agencies and the SSA to verify the income of an applicant or beneficiary of the AFDC, SSI, and food stamp programs. (Presently, IRS is required to disclose only information on earned income.) The Deficit Reduction Act also requires States to maintain a system of quarterly wage reporting as part of its income verification system.

SOURCE: Office of Technology Assessment.

sional authorizations of computer matching place agencies in a position where the legitimacy of either a disclosure or refusal to disclose can be challenged. A prime example is *Tierney v. Schweiker*, 718 F.2d 449 (1983), which involved the Social Security Administration's (SSA) use of confidential tax return information maintained by IRS for purposes of verifying the income and assets of supplemental security income recipients. SSA was acting on its congressional mandate that SSA's determinations of eligibility be based on "relevant information [that is] verified from independent or collateral sources and additional information [that is] obtained as necessary."[24] Two GAO reports[25] recommended that SSA use IRS tax information to verify eligibility. In deciding the case, Judge Abner Mikva recognized that:

> Much of the confusion . . . arises from conflicting signals given by the Congress. In 1972, when enacting the Social Security Amendments that instituted the Benefits program, Congress was concerned with ensuring that financially ineligible individuals not abuse the system. To this end, Congress directed the SSA to obtain as much information as possible to discover such ineligibility. In 1976, when expanding the confidentiality provisions as part of the Tax Reform Act of 1976, Congress made clear that tax information was to be absolutely confidential, subject to certain explicit exceptions. Although Congress created numerous exceptions, none was applicable to the information which SSA now seeks. When Congress speaks with two separate minds, the conflicting goals can present difficult dilemmas.[26]

In response to the OTA survey, 43 percent of agency components that reported participation in computer matching activities (16 out of 37) said that the matches were required or authorized by legislation. However, approximately one-third of the respondents cited general statutes such as an Inspector General Act, the Debt Collection Act, or an Omnibus Reconciliation Act. Another one-third cited explicit requirements for matching, such as the Uniform Code of Child Support or Title 7, U.S.C., chapter 51, "Food Stamp Program." Another one-third cited more general authorization, e.g., Public Law 96-473, which requires the suspension of benefits for inmates of penal institutions and is given as the basis for matches between inmate records and social security files.

Finding 2

It is difficult to determine how much computer matching is being done by Federal agencies, for what purposes, and with what results. However, OTA estimates that, in the 5 years from 1980 to 1984, the number of computer matches nearly tripled.

---

[24] 42 U.S.C. sec. 1383(3)(1)(B) as quoted in *Tierney v. Schweiker* 718 F.2d 449, 451 (1983).

[25] U.S. General Accounting Office, HRD 81-4, Feb. 4, 1981 and HRD 82-9, Jan. 12, 1982.

[26] *Tierney v. Schweiker* 718 F.2d 449, 454 (1983).

There has been no accurate accounting of the number of matches that have been done at the Federal level. In part, this is a definitional problem. One distinction that affects reports of the amount of computer matching being done is that of "matching programs" versus "matches." The OMB guidelines define a "matching program" as:

> . . . a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants.[27]

Based on this definition, there will be many more matches than there are matching programs, as one matching program may include a number of record sets (e.g., Office of Personnel Management (OPM) records with SSA records and OPM records with Farmers' Home Administration loans), and/or a matching program may involve a number of matches at certain intervals, e.g., yearly or monthly. However, this distinction between matching programs and matches has not always been recognized in accounts of numbers of computer matches.

A second important distinction in understanding reports on the scale of computer matching by Federal agencies is one made by OMB. Some compilations of computer matching at the Federal level include only those matches that fall under the OMB guidelines, others include both, and still others do not differentiate. OMB's guidelines state that the following are not matching programs:

1. Matches that do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan database with the OPM's Federal Employee database, would be covered; comparison of six individual student loan defaultees with the OPM file would not.
2. Checks on specific individuals to verify data in an application for benefits, done soon after the application is received.
3. Checks on specific individuals based on information that raises questions about an individual's eligibility for benefits or payments, done reasonably soon after the information is received.
4. Matches done to produce aggregate statistical data without any personal identifiers.
5. Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.
6. Matches done by an agency using its own records.[28]

For the purposes of this report, the first three applications are considered front-end verification and are discussed in chapter 4. The fourth and fifth applications are not relevant to this inquiry. The sixth application does include a significant number of matching programs and matches that are relevant to this discussion, e.g., SSA and another component of the Department of Health and Human Services.

In addition to definitional problems, the rules for reporting matches may not require that all matches be reported. Notices of computer matching programs that meet the criteria in the OMB guidelines may appear in the *Federal Register* as a new routine use. However, if the agency providing the data believes that the system of records already contains such a use, then no additional notice in the *Federal Register* is required. No notice is required for records that are matched within an agency.

There have been a number of attempts at determining the scale of computer matching. Figures range from 200 programs on upwards.

---

[27] Office of Management and Budget, "Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs," *Federal Register*, vol. 47, No. 97, May 19, 1982, p. 21657.

[28] Ibid., p. 21757.

For example, in 1982 hearings on computer matching, Senator William Cohen estimated that:

> As of January 1982, Federal agencies had completed more than 85 matching programs and State government agencies are now performing approximately 170 matches involving public assistance records, unemployment compensation records, government employee files, and in some cases, the files of private companies. These projects involve the records of hundreds of thousands of citizens.[29]

At the same hearings, Thomas McBride, former Inspector General of the Department of Labor, testified:

> So my guess is we are talking about a population of roughly 500, more or less, routine recurring matches going on, some of them subject to Federal legislative action, some of them not.[30]

The Long Term Computer Matching Project of the President's Council on Integrity and Efficiency has issued three compilations of Federal computer applications to prevent/detect fraud, waste, and abuse. These compilations do not provide complete listings of computer matching programs.[31] They include those computer matches that agencies chose to report; some agencies submitted partial reports, others appear not to have responded at all, or to only one or two of the PCIE's requests. Some of the reported matches are one time only, others are recurring. The first compilation was distributed in 1982[32] and reported 77 matches; the second was distributed in July 1984 as an expansion and update, and reported 162 matches; and the third was distributed in January 1986 as an update, and reported 108 matches.[33] (See table 8 for breakdown by agency.)

A 1985 GAO study, *Eligibility Verification and Privacy in Federal Benefit Programs: A Delicate Balance,* reported that:

> Before 1976, only two benefit program-related Federal computer matching projects were conducted. However, recent inventories of Federal and State agencies' computer matching programs show that Federal agencies had initiated 126 benefit-related matches, 38 of which were recurring as of May 1984. State agencies, as of October 1982, had initiated more than 1,200 matching projects, most of them recurring.

Table 8.—Computer Matches Reported to the PCIE Long-Term Computer Matching Project

	1982	1984	1986
Department of Agriculture	11	10	23
Department of Commerce	0	1	1
Department of Defense	0	30	0
Department of Education	1	1	0
General Services Administration	1	1	18
Department of Health and Human Services	29	58	55
Department of Housing and Urban Development	0	4	3
Department of the Interior	0	1	0
Department of Justice	8	5	0
Department of Labor	12	12	0
National Science Foundation	0	2	0
Nuclear Regulatory Commission	0	1	0
Peace Corps	0	1	0
Pension Benefit Guaranty Corp.	0	1	0
Office of Personnel Management	3	5	0
Railroad Retirement Board	0	8	1
Small Business Administration	1	1	0
Department of State	2	2	0
Tennessee Valley Authority	0	4	5
Department of the Treasury	0	3	0
Veterans Administration	9	11	2

SOURCE: President's Commission on Integrity and Efficiency.

---

[29] Cohen hearings, op. cit., p. 2.

[30] Ibid., p. 20.

[31] It does not appear that the PCIE inventory used the OMB guidelines' definition of computer matching programs. Some agencies reported matches within their agency, e.g., Department of Health and Human Services Black Lung and SSA Title II. Some agencies reported particular matches within a matching program.

[32] None of the compilations is dated. The phrase "distributed in 1982" is used by PCIE in its second compilation to describe the first compilation.

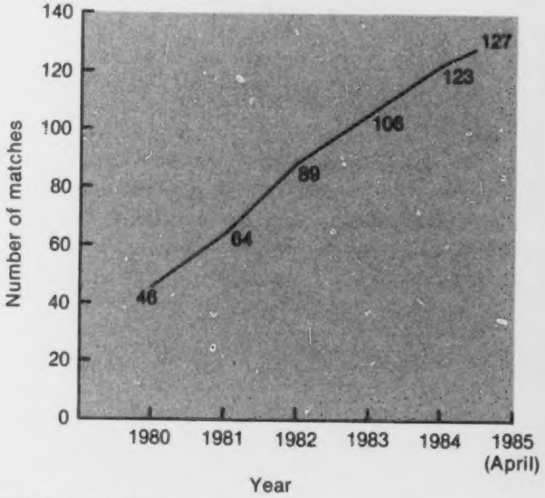
[33] The low figures in the 1986 compilation can be attributed to two factors. The first is that some large agencies that previously had reported a number of matches did not respond, e.g., Departments of Labor, Defense, and Justice. The second factor is that many agencies have increased their use of computer screens and profiles rather than their use of computer matches. This latter factor will be discussed in ch. 4.

In response to the OTA survey of Federal agencies, 11 cabinet-level departments and 4 independent agencies reported conducting 110 matching programs[34] with a total of approximately 700 matches from 1980 to April 1985. The Departments of Energy and State were the only two cabinet-level departments that reported no matching programs. Of the 20 independent agencies surveyed, only three (NASA, Selective Service System, and Veterans Administration) reported any matching programs (see table 9 for a breakdown of matching programs by agency).

While the data from the responses to OTA and to PCIE are not directly comparable, the trend toward increased use of computer matches is clear (see figure 4). In the 5 years from 1980 to 1984, the number of computer matches nearly tripled.

From 1979 to 1984, OMB received only 56 reports on matching programs from Federal agencies. According to OMB records, there were 11 matches reported in 1979; 2 in 1980; 11 in 1981; 13 in 1982; 6 in 1983; and 13 in 1984. The OMB figures are obviously lower than the matching figures reported elsewhere because: 1) only those matching programs that fit the OMB definition are included; and 2) some agencies do not submit match notices under the routine use and systems of records, but instead fit matching programs into existing routine use and existing systems of records.

Figure 4.—Computer Matches Conducted From 1980 to April 1985



SOURCE: Office of Technology Assessment.

Table 9.—Computer Matching Programs[a] Reported to OTA

Department of Agriculture	33
Department of Commerce	1
Department of Defense	15
Department of Education	3
Department of Health and Human Services	1
Department of Housing and Urban Development	3
Department of the Interior	3
Department of Justice	6
Department of Labor	21
Department of Transportation	1
Department of the Treasury	14
National Aeronautics and Space Administration	1
Selective Service	1
Veterans Administration	7

[a] Some of these matching programs are conducted within an agency and therefore do not fall within the OMB definition.

SOURCE: OTA Federal Agency Data Request.

In determining the scale of computer matching activities at the Federal level, it is also important to consider the number of records that have been matched. In response to the OTA data request, information on number of records matched, number of hits, and percent of hits verified was provided for 20 percent of the matches reported. Despite this low response, the number of separate records used in the reported matching programs totaled over 2 billion; the total number of records matched was reported to be over 7 billion due to multiple matches of the same records.

---

[34] Some of these matching programs are conducted within an agency and therefore do not fall within the OMB definition.

Finding 3

As yet, no firm evidence is available to determine the costs and benefits of computer matching and to document claims made by OMB, the inspectors general, and others that computer matching is cost-effective.

Before discussing the attempts to date at estimating costs and benefits, it is important to place computer matching within a context. Computer matching is a technique that has been used primarily to detect client fraud, which is only one component of fraud, waste, and abuse. In order to accurately determine the cost-effectiveness of computer matching, the extent of client fraud must first be documented. If client fraud accounts for only a small percentage of total fraud, waste, and abuse, then other techniques to detect other types of fraud, waste, and abuse may be more cost-effective overall. In this respect, one author cited the 1978 Annual Report of the HEW Inspector General, which estimated that the Department lost between $5.5 and $6.5 billion through management inefficiencies, program misuse, and fraud. In this instance, management inefficiencies and program misuse accounted for 97 percent of the inspector general's estimate of losses, while client fraud accounted for only 3 percent.[35]

In response to the OTA survey, only 8 percent of the agencies that reported participation in computer matching activities (3 out of 37 agencies) said that they did cost-benefit analyses prior to computer matching. Eleven percent (4 of 37) reported doing cost-benefit analyses after matching.

Various individuals and organizations have asserted that computer matching is cost-effective, but have provided little or no specific information on actual costs and benefits. For example, Joseph Wright, OMB's Deputy Director, reported in an OMB circular that:

> The IG's are wisely using this spectacularly effective technique to reap for the American public the savings that private industry has for many years been obtaining. Use of this technique will help assure that individuals who are not entitled to receive payments don't, making more money available for those who are deserving.[36]

Likewise, the Grace Commission concluded that:

> Computer matching is an effective management tool for identifying fraud, waste, and abuse of government benefits, entitlements and loan programs. Computer matching is useful in other ways too, such as validating billings of large government contractors. . . Recommendations in the task force reports to correct information problems related to this issue provide opportunities for cost savings and revenue of $15.9 billion over 3 years ($11.3 billion when information gaps cited in other issues in the Report are netted out).[37]

In the 1982 Cohen hearings on computer matching, former Inspector General McBride of the Department of Labor testified that:

> The hits, the overpayments, for the big benefit programs run somewhere between 1.8 up to maybe 4 percent, depending on what program you are talking about. For AFDC, the hits are probably somewhere at the lower end, because they do a little better job of verification. Food stamps is a little higher. Unemployment insurance may be even higher, in some States particularly.[38]

In a 1983 article, Richard Kusserow, Inspector General of the Department of Health and Human Services, reported:

> Our own Project Spectre which matches Social Security beneficiary payments with Medicare death files has led to about $7.5 million in recoveries to date. Recoveries, in this case, covers all monies collected by our investigators, including checks not cashed but debited to the treasury. We project total savings over time to reach $25.2 million.[39]

In *Computer Matching in State Administered Benefit Programs: A Manager's Guide*

---

[35] Young, op. cit., p. 362.

[36] OMB 83-14.

[37] President's Private Sector Survey on Cost Control, *A Report to the President* (1984), Part II: Issue and Recommendation Summaries, p. 82; see pp. 84-86 for examples.

[38] Cohen hearings, op. cit., p. 19.

[39] Richard P. Kusserow, "Fighting Fraud, Waste and Abuse," *The Bureaucrat*, fall 1983, p. 23.

to Decision Making,[40] the quantitative benefits of computer matching include estimated savings and measures of grant reductions, collections, and corrections. The list of qualitative benefits is longer, including: increased deterrence, improved eligibility determinations, enhanced public credibility for benefit programs, more effective referral services, and improved databases.

The costs of computer matching vary according to the size of the record set, as well as the complexity, quality, and compatibility of the records. In *Computer Matching in State Administered Benefit Programs,* the quantitative costs include: hardware/software; computer processing time; space; supplies; personnel managers, data-processing staff, eligibility assistance workers, clerical workers, hearings officers, fraud investigators, collections staff, attorneys, and training staff; other public agency resources; and private institution resources. The qualitative costs include: reduced staff morale, heightened public concerns about "big brother," increased political conflict, gamesmanship with numbers, operational inefficiencies, and diversion of resources. Definitions for these qualitative costs are not offered.

All agree that verification costs are the highest and the most difficult to compute. In *Computer Matching in State Administered Benefit Programs,* it is pointed out that:

> Follow-up is the most costly, labor-intensive part of the computer matching process. Most notably, it involves what can be a very tedious and time-consuming job of verifying hits. But it also involves other components such as making any necessary change in a recipient's case status, calculating and pursuing overpayments, hearing appeals, making referrals to fraud units, and actually conducting criminal investigations and pursuing convictions.[41]

There is some disagreement as to how much verification, both in terms of number of hits verified and in terms of records and sources checked, is necessary. For example, the Department of Health and Human Services' Inspector General Kusserow has suggested that:

> For large matches, officials would have to analyze only a sample of the hits to verify the matching process. After doing this, officials should take corrective measures, proceeding cautiously against any individual where doubt exists.[42]

The PCIE Long Term Computer Matching Committee has developed some information on the costs of selected matches. For many of the matches, the information presented is very sketchy. The matches for which the PCIE offered the most complete information are listed in table 10.

David H. Greenberg and Douglas A. Wolf have recently completed a study[43] in which they constructed a cost-benefit framework (see table 11) and used it to evaluate the performance of computer wage-matching systems of welfare agencies in four areas: Camden County, New Jersey; Mercer County, New Jersey; San Joaquin County, California; and the State of New Hampshire. In each of their study sites, they reported that they obtained reliable and complete information on the costs of matching, but were unable to measure benefits as precisely. Additionally, there were some benefits, e.g., deterrent effects and positive effects on attitudes of affected parties, that they could not measure at all. Thus, they regard their test of the cost-effectiveness of wage matching to be a conservative one.

Greenberg and Wolf concluded from their four case studies that the benefits from computer matching outweighed the costs by "substantial amounts"[44] (see table 12). If computer matching were as effective nationally, they suggested that "cost savings in the food stamp and AFDC programs would be approximately

---

[40] U.S. Department of Health and Human Services, Office of Inspector General, *Computer Matching in State Administered Benefit Programs,* June 1984, p. 25.

[41] Ibid.

[42] Richard P. Kusserow, "The Government Needs Computer Matching To Root Out Waste and Fraud," *Communications of the ACM,* vol. 27, No. 6, June 1984, p. 544.

[43] David H. Greenberg and Douglas A. Wolf, "Is Wage Matching Worth All the Trouble?" *Public Welfare,* winter 1985, pp. 13-20.

[44] Ibid., p. 18.

Table 10.—Examples of Cost/Benefit Analyses

Costs/benefits	Selected matches					
	DOL/TVA	IRS/DOL	OPM/SSA	OPM/OPM	RRB/HCFA	USAF/VA
Equipment costs	1,500	125,000	10,950	2,291	6,124	1,000
ADP staff costs	1,200	25,000	3,213	2,142	1,831	1,150
Staff verification costs	4,500	1,000,000	94,163	12,968	15,763	96
Travel and other costs	10,000	—	39,416	—	10,028	100
Cases found	21	219	770	170	405	340
Overpayments identified	35,000	103,000	9,100,000	640,800	2,263,927	71,000
Cases with recoveries made	2	219	—	—	364	—
Overpayments recovered	2,500	139,000	—	—	993,118	—
Overpayments prevented	—	—	770	170	—	1,300
Amount prevented	—	50,000	4,089,600	46,300	—	274,000
Questioned costs	—	—	—	—	—	—
Disallowed costs	—	—	—	—	—	—

KEY: DOL = Department of Labor; TVA = Tennessee Valley Authority; IRS = Internal Revenue Service; OPM = Office of Personnel Management; SSA = Social Security Administration; RRB = Railroad Retirement Board; HCFA = Health Care Financing Administration; USAF = U.S. Air Force; VA = Veterans Administration.

SOURCE: President's Council on Integrity and Efficiency Long Term Matching Committee, "Draft/Summary of Federal Computer Applications for Prevention of Fraud and Abuse."

Table 11.—Costs and Benefits of Wage Matching

Benefits:

Restitution of previous overpayments
Savings from food stamp disqualifications
Savings from benefit reductions and discontinuances:
- prevention of future overpayments
- administrative savings

Changes in behavior and attitudes:
- deterrent effects
- improved client attitudes
- improved staff morale
- improved relations with the public

Costs:

Personnel costs (salaries and fringe benefits):
- income maintenance staff
- fraud investigative staff
- district attorney staff
- other

Materials and facilities costs:
- computers
- word processors
- forms
- general overhead such as office space, telephone, supplies

SOURCE: David H. Greenberg and Douglas A. Wolf, "Is Wage Matching Worth All the Trouble?" *Public Welfare*, winter 1985, p. 16.

Table 12.—Estimated Costs and Benefits of Computer Matching in Four Sites

	Costs	Benefits	Ratio
Mercer County	$786,821	$ 932,958	1.19
Camden County	753,662	1,452,367	1.93
San Joaquin County	308,128	762,355	2.47
New Hampshire (DES Wage Crossmatch Project)	264,856	707,316	2.67

NOTE: All figures are in annual terms pertaining mainly to 1982.

SOURCE: David H. Greenberg and Douglas A. Wolf, "Is Wage Matching Worth All the Trouble?" *Public Welfare*, winter 1985, p. 18.

1 or 2 percent."[45] However, they caution that this may not be the case because they chose wage-matching programs that were functioning well:

> For example, the employer-reported data used by these systems clearly were adequate in terms of coverage, content, and timeliness. Equally important: follow-up procedures were well-structured, adequate resources were available for follow-up, and supervisors were genuinely committed to the program. Without such conditions, it certainly is possible that wage matching could prove ineffective.[46]

Finding 4

The effectiveness of computer matches that are used to detect fraud, waste, and abuse can be compromised by inaccurate data.

The Massachusetts case discussed earlier, in which 110 of the 160 termination notices that were sent following a computer match were based on erroneous information, is the best known example of use of inaccurate data. However, many matches experience some problems with inaccurate data, and, in part, computer matching can be effective in detecting errors in data.

---

[45] Ibid.

[46] Ibid.

One indicator, although not complete, of the quality of data used in computer matching is the percentage of hits verified as accurate. In response to the OTA survey, this percentage ranged from 0.1 to 100 percent. For example:

- The Department of Housing and Urban Development conducted computer matches to identify tenants in five different cities who had not reported all income when applying for federally assisted housing. The hit rates varied from about 6 to 54 percent, and the hit verification rates varied from 13 to 55 percent. The actual number of matches that resulted in valid hits ranged from 0.8 to 29 percent.
- The Department of Commerce Inspector General's office conducted a match to identify departmental employees who were collecting unemployment benefits. A total of 22,000 records were matched resulting in 98 hits, of which about 10 percent were verified.
- The Department of Education conducted a match to identify current and former Federal employees who were delinquent on student loans. About 10 million records were matched resulting in 46,860 hits, of which 100 percent were verified, according to Department officials.
- The Veterans Administration conducted a match to identify Federal employees and annuitants who were erroneously receiving VA compensation. About 15 million records were matched resulting in 5,166 hits, of which about 23 percent were verified.

For the majority of matches reported to OTA, information on hits verified was either unknown or unavailable.

Proponents of matching programs are taking measures to improve the quality of data used in matches. SSA has developed a computer software program to screen social security numbers and pull out inaccurate or incongruous numbers. Other agencies engaging in matching programs are likewise concerned. In response to the OTA survey, 68 percent (25 of 37) of the agencies indicating that they participated in matching programs said that procedures were used to ensure that the subject record files contain accurate information.

Finding 5

There are numerous procedural guidelines for computer matching, but little or no oversight, follow-up, or explicit consideration of privacy implications.

Program personnel appear to have substantial discretion in deciding whether or not to use computer matching as an audit technique or means to detect fraud, waste, and abuse. There are few internal agency checks. The Inspector General's Office may be involved in planning a computer match; and the General Counsel's Office and the Privacy Act officer may be involved. But it appears that there are no agency or general policy guidelines regarding what types of information should be matched, against which records of what other agencies, and for what purposes. These substantive issues are rarely addressed.

For those matching programs that meet the OMB definition, agencies providing information "are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure when they do." In making this determination, agencies are instructed to consider the following:

- legal authority for the match;
- purpose and description of the match;
- description of the records to be matched;
- whether the record subjects have consented to the match; whether disclosure of records for the match would be compatible with the purpose for which the records where originally collected, i.e., whether disclosure under a "routine use" would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity; or any other provision of the Privacy Act under which disclosure may be made;
- description of additional information that may be subsequently disclosed in relation to "hits";

- subsequent actions expected of the agency providing information (e.g., verification of the identity of the "hits" or follow-up with individuals who are "hits"); and
- safeguards to be afforded the records involved, including disposition.

However, neither the source agency, the matching agency, nor OMB is accountable for the decision whether or not to disclose records for a matching program. For matching programs that do not fall under the OMB guidelines, there are no formal procedures or guidelines—one program manager may ask another for access to records for matching purposes, and no one else need know.

OMB has developed a number of procedural guidelines. The initial guidelines, *OMB Guidance to Agencies on Conducting Automated Matching Programs,* became effective on March 30, 1979. The purpose of the guidelines was "to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy." Under the guidelines, a match was to be performed "only if a demonstrable financial benefit can be realized that significantly outweighs the costs of the match and any potential harm to individuals that could be caused by the matching program." To this end, the guidelines required documentation of benefits, costs, potential harm, and alternatives considered to detect or curtail fraud and abuse or to collect debts owed to the Federal Government (see 5a of guidelines for listing). A report describing the match (see 9b.1 and 2 of guidelines for details) was to be submitted, 60 days before the match was initiated, to the Director of OMB, the Speaker of the House, and the President of the Senate. Necessary notices of system of records, new or altered systems, or routine use were to be published in the *Federal Register,* allowing 30 days for public comment. Any disclosures of personal information during the match were to be made in accordance with the "routine use" limitations noted in the *Federal Register.* Unless it was a continuing matching program, the guidelines stipulated that personal records should be destroyed or returned to the source agency within 6 months. The guidelines also suggested that matching should be done inhouse by agency personnel, not by contractors.

The application of these guidelines was not very satisfactory for any party concerned. Agencies did not conduct cost-benefit analyses in a systematic fashion; instead, they were quickly estimated when asked for by OMB in order to comply with the letter of the guidelines. There was almost no public comment in response to matches proposed in the *Federal Register.* There was little congressional reaction to matching programs. There was minimal to no oversight by OMB; it processed the necessary paperwork, but never "disapproved" a match. In part, OMB's behavior can be attributed to the lack of clarity in the guidelines concerning its role. For example, it was not clear from the guidelines whether OMB had the authority to disapprove a match.

Based on the unsatisfactory experience under the 1979 guidelines, the PCIE's Long Term Computer Matching Project decided that one of its first projects would be to revise the OMB guidelines. In conjunction with advice from PCIE, OMB's *Revised Supplementary Guidance for Conducting Matching Programs* became effective May 1, 1982. The 1982 guidelines simplified the administrative reporting requirements of the 1979 guidelines by eliminating the cost-benefit analysis, reducing the notice and reporting requirements, and exempting intra-agency matching programs. Publication of "routine uses" in the *Federal Register* was still required, but the 30-day public comment period for matching reports and advance notice to Congress and OMB were eliminated.

OMB and PCIE also developed a *Model Control System for Conducting Computer Matching Projects Involving Individual Privacy Data (1983).* The Model Control System is designed to provide procedural guidance to agencies conducting computer matching projects to help them comply with the Privacy Act and the OMB guidelines. The model includes 10 steps that agencies should follow:

1. define the match program,
2. determine the feasibility of the match,
3. establish matching and follow-up procedures,
4. confer with the agencies providing information,
5. publish routine use notice,
6. make a matching report,
7. obtain the agency data file,
8. conduct computer matching,
9. analyze and refine the raw hits, and
10. perform follow-up procedures.

Agencies are not required to follow the Model Control System, or to report to OMB on which procedures were followed.

In late 1983, OMB developed a *Computer Match Checklist* that must be on file for review by OMB, GAO, or other Federal entities. The checklist must be completed by both the agency providing information and the agency conducting the match immediately following *Federal Register* publication of an intent to match. Items on the checklist include: compliance with notification requirements, number of individuals whose records are to be matched, contractor involvement, and the date on which a cost/benefit analysis on the match will be available. Estimates of cost/benefit analyses are to be attached to the checklist.

In December 1985, OMB issued Circular A-130, *Management of Federal Information Resources*, which directs agencies to review annually every matching program in which they have participated, either as a matching or source agency, to ensure that the requirements of the Privacy Act, the OMB Matching Guidelines, and the OMB Model Control System and Checklist have been met. Additionally, agencies are to include in the Privacy Act Annual Report the number and description of matching programs participated in as a source or matching agency.

Finding 6

As presently conducted, computer matching programs may raise several constitutional questions, e.g., whether they violate protection against unreasonable search and seizure, due process, and equal protection of the laws. But, as presently interpreted by the courts, the constitutional provisions provide few, if any, protections for individuals who are the subjects of matching programs.

The fourth amendment provides individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The fourth amendment presumption, reinforced by case law and by the presumption of innocence additionally reflected in the fifth and sixth amendments, is that searches are not warranted unless there is indication of a crime. If there is probable cause of a crime and the individual's involvement, then a court may issue a search warrant. Fourth amendment case law has resulted in the concept of "expectation of privacy."

The question of whether or not computer matches raise fourth amendment issues turns, in large part, on the "expectation of privacy" that individuals have in records about them maintained by a third party, in this case primarily a government agency. Based on the Supreme Court's ruling in *United States v. Miller*, 425 U.S. 435 (1976), records that are held by a third party, and used by that party for administrative purposes, are considered the property of the third party. Under such circumstances, the individual does not have an assertible fourth amendment privacy interest in those records. Although *Miller* applied to records held by a bank, the logic of the holding may apply similarly to records held by the government.

In *Jaffess v. Secretary HEW*, 393 F. Supp. 626 (S.D. N.Y. 1975), a district court allowed a computer match of recipients of veterans' disability benefits with those receiving social security benefits. The court held that the disclosure under the matching program was "for the purpose of proper administration." Jaffess had not reported his social security income, and after the match his veterans' benefits were reduced. He claimed that a constitutional right of privacy protected his records. The court rejected this claim:

> . . . the present thrust of decisional law does not include within its compass the right of an individual to prevent disclosure by one governmental agency to another of matters obtained in the course of transmitting agency's regular functions.[47]

But, the legal question of what kind of fourth amendment "expectation of privacy" an individual has when he or she fills out a form and swears that the information provided is true and correct has not been specifically decided. Nor has the question of the privacy rights of Federal workers in information provided and maintained for employment purposes. In both instances, statutes, especially the Privacy Act, may give more precise legal guidance than the U.S. Constitution. However, the constitutional question could still be subject to further litigation.

A second fourth amendment issue that is raised by computer matches is the scope of the search. Computer matches are general electronic searches of, frequently, millions of records. Under the fourth amendment, searches are not to be overly inclusive—no "fishing expeditions" or "dragnet investigations." Yet, in matches, many people who have not engaged in fraud are subject to the computer search. If matches were to be considered a fourth amendment search, then some limitations on the breadth of the match and/or justifications for a match may be necessary. For example, the agency may need to show that a less intrusive means to carry out the search was not available, and that procedural safeguards limiting the dangers of abuse and agency discretion were applied. These may also be required under due process protections as discussed below.

A final fourth amendment issue that may be raised by computer matches is that of suspicion that criminal activity is occurring. If the purpose of a match is to produce evidence that someone has defrauded the government, then a computer match could be regarded as a search under the fourth amendment. Such a match may also conflict with the presumption of innocence, as reflected in the fourth and fifth amendments, if the individual is required to prove that he or she has not engaged in wrongdoing. If the purpose of a match is to detect and correct errors, and not to detect wrongdoing, then a match would probably not be regarded as a search under the fourth amendment.

The *due process* clause of the fifth[48] (Federal Government) and 14th (State governments) amendments ensures procedural protections before the government takes action against an individual. Generally, this clause has been held to require that individuals be given notice of their situation, the opportunity to be heard, and the opportunity to present evidence on their own behalves. In agency proceedings, this constitutional principle is given specific meaning in the Administrative Procedures Act (1946). Additional elements of due process that apply specifically to eligibility for benefit programs include: the right to a pre-termination hearing, placing the burden of proof on the government to prove ineligibility if the individual swears to eligibility, and entitlement to benefits pending resolution. These procedural due process protections were extended to welfare recipients in *Goldberg v. Kelly*, 397 U.S. 254 (1970).

Under the 1979 OMB guidelines, notice of a proposed match is to be published in the *Federal Register* 30 days before to allow time for comments. Many have questioned the adequacy of this, as the vast majority of individuals do not read the *Federal Register*. Additionally, there is evidence that agencies have not complied with the 30-day time period and that some agencies have provided notice *after* the match was well under way.[49] This requirement was eliminated in the 1982 OMB guidelines. DEFRA now requires more specific notice prior to some matches. It is important to recognize that notice can take place at various points in the matching process, i.e., before the match occurs, once an individual appears as a "hit," and prior to any outside verification. Notice can also be provided rather passively, e.g., a statement on a form, or requiring the active acknowledgment of the individual. Based on results of the OTA survey, 8 percent (3 out of 37 agency components) of the agencies reporting that they participated in computer matching said that individual subjects of the match had provided written consent prior to a match.

---

[47] Kenneth James Langan, "Computer Matching Programs: A Threat to Privacy?" *Columbia Journal of Law and Social Problems*, vol. 15, No. 2, 1979, pp. 158-159.

[48] It does not specifically provide for equal protection, but the Court ruled in *Bolling v. Sharpe* (347 U.S. 497, 19854) that "the concepts of equal protection and due process, both stemming from our American ideal of fairness, are not mutually exclusive" and that the fifth amendment also provided equal protection.

[49] See Cohen hearings, op. cit.

Once a match has taken place, the resulting "hits" are further investigated in order to verify their status. At this time, these individuals may not be given notice of their situation, or the opportunity to be heard and present evidence on their own behalves. They may not be notified until and unless the agency decides to take some action against them. Based on the Court's ruling in *Goldberg*, due process would require a hearing for an individual whose benefits are to be terminated or lowered based on information from computer matching. Such hearings may be quasi-judicial in nature, but the individual would not have the right to a lawyer or jury, the burden of proof would be on the individual, and the individual may incriminate himself or herself in these hearings. If such hearings are the starting point for an investigation leading to criminal charges, then it may be necessary to conduct them in a more formal judicial setting.

The *equal protection* clause of the 14th and, by implication, the fifth amendments prohibits the States and Federal Government from creating legal categories and taking actions that discriminate against members of that category (e.g., race, national origin, and gender). Economic status has never been regarded as a suspect classification,[50] and therefore the government's interest in subjecting welfare recipients to computer matching would only need to be rationally related to a legitimate purpose of the government. In this case, the purpose, i.e., detecting fraud, waste, and abuse, would probably be regarded as legitimate, and the means chosen, i.e., computer matching, rationally related.

Despite this development of constitutional decisions, matching may conflict with the equal protection clause in that categories of people, not individual suspects, are subject to these electronic searches. In the computer matching that has been done to date, two groups of people—welfare recipients and Federal employees—have been used frequently. This is true despite arguments by supporters of matching that computer matches are effective tools in a number of situations. Although the Grace Commission and others have recognized the usefulness of matching in detecting fraud, waste, and abuse in government contracting, it has not been used to any significant extent for this purpose. DEFRA, in its section incorporating the Grace Commission recommendations, did not require or endorse the use of matching in government contracting.

Finding 7

The Privacy Act as presently interpreted by the courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.

The Privacy Act gives individuals certain rights of notice, access, and correction in order that they may control information about themselves. It also places certain requirements on agencies to make certain that the information they maintain is relevant, timely, and complete.

Under the Privacy Act, the individual has the right to prevent information being used without his or her consent for a purpose other than that for which it was collected. An exception to this rule is if information falls within a "routine use" of the particular record system. Under the OMB Matching Guidelines, matching can be considered such a routine use; therefore, individual consent is not required. Many argue that matching of information is not consistent with the legislative intent that information should be used only for the purpose collected. As table 6 indicated, it is quite easy to find justification in the Privacy Act for disclosures of information for matching purposes.

---

[50] See *Dandridge v. Williams*, 397 U.S. 471 (1970) and *San Antonio Independent School District v. Rodriguez*, 411 U.S. 1 (1973).

Additionally, the Privacy Act requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs" [sec.e(2)]. In computer matching, information that will be used to determine whether benefits should be eliminated, decreased, or increased is collected from third parties—not from the individual.

Although not specifically prohibited in the Privacy Act, the legislative history reflects censure of a national data center. The linking of systems in computer matching can be regarded as moving towards a *de facto* national data center or national recipient system. Additionally, new computerized databases are being created solely for the purpose of providing information for computer matches and other record searches. The Federal Government, under the auspices of the inspectors general, is developing a national computerized file of deceased individuals (who have no rights under the Privacy Act) for screening beneficiary records and preventing payments to deceased persons. Two other examples mentioned previously are the Medicaid Management Information System and the proposed IRS Debtor Master file. The State wage reporting systems, required under the proposed DEFRA regulations, could also be regarded as the first stage of a national data system.

The OMB guidelines require that the files used for matching be returned to the custodian agency or destroyed. However, since there is no oversight of this, records could be used for additional purposes.

Finding 8

The courts have been used infrequently as a forum for resolving individual grievances over computer matching, although some organizations have brought lawsuits.

It does not appear likely that the courts will protect individual privacy in computer matching programs.[51] There are at least four reasons. The first is that the courts have not extended constitutional protections for computerized records, and the fourth amendment "search and seizure" doctrine has not been applied. The second reason is that courts only require rationality in such programs, i.e., that the means used be reasonably related to a legitimate government purpose. The purpose of achieving efficiency and detecting fraud, waste, and abuse is a legitimate one. With respect to the choice of means, courts have traditionally given deference to administrative discretion. The third reason is that when courts balance individual privacy against the public interest, the weight generally favors the public interest—all else being equal. The fourth reason is that the damage requirements of the Privacy Act are so difficult to prove that they act as a deterrent to its use.

Additionally, with large-scale computer matching, no one individual is sufficiently harmed to litigate a claim and most individuals are not even aware of the match. The cases that have gone to court have generally been brought by welfare rights organizations. These cases include:[52]

> *15, 844 Welfare Recipients v. King*, 474 F. Supp. 1374 (D.Mass., 1979)—State welfare agency was required to restore benefits to recipients whose aid had been terminated either by fraud investigators improperly acting as caseworkers, or by caseworkers improperly acting as fraud investigators.
>
> *Tierney v. Schweiker*, 718 F. 2d 449 (D.C. Cir., 1983)—Coerced signatures to notice-and-consent forms, extracted from SSI recipients in preparation for an IRS matching, were invalidated because the agency action violated IRS confidentiality rules.

---

[51] Langan, op. cit., p. 175.

[52] See: Henry Korman, "Creating the Suspicious Class—Surveillance of the Poor by Computer Matching," unpublished paper, August 1985, esp. pp. 52-53.

Greater Cleveland Welfare Rights Organization v. Bauer, 462 F. Supp. 1313 (N.D. Ohio, 1978)—An Ohio wage match was invalidated insofar as subject AFDC recipients were not informed of use of their social security numbers as identifiers in the match.

Lessard v. Atkins, CA 82-3389-MA (D. Mass., Apr. 23, 1985)—Defendants in a bank match case agreed to both the use of secondary identifiers and enhanced follow-up investigations that plaintiffs argued were required by Federal law.

Finding 9

Computer matches are conducted in most States that have the computer capability. At least four-fifths of the States are known to conduct computer matches, most in response to Federal directives.

In many respects, the personal information gathered by State agencies is more sensitive and more extensive than that gathered by Federal agencies.[53] Many Federal agencies fund programs that are administered through the States (or local educational agencies). The Federal agencies do not store individually identifiable information on all of the beneficiaries of these programs, but the States do. Federal auditors regularly have access to individually identifiable information to monitor program effectiveness, but the personal data on all participants is not stored in Federal agencies themselves.

At the State level, the following information is typically stored: income or business taxpayer records in the revenue department; driving records in the Department of Motor Vehicles; public assistance in the welfare agency; drug and alcohol treatment records in the appropriate agencies; communicable diseases and abortions in the Department of Health; treatment at State institutions in the Departments of Health, Mental Health, or Public Health; current earnings in the quarterly reports submitted by employers (a few States require reporting less often) to the unemployment security office; criminal records and criminal intelligence in the State police or Department of Public Safety; educational, financial aid, and vocational training information in the Department of Education; occupational information in the various State licensing boards (attorneys, beauticians, auctioneers, boxers, vendors, physicians, etc.); patient information and physicians' earnings records in the State agency administering Medicaid; suspicions of child abuse in the appropriate State agency; and birth records of adoptees in the adoption agency.

Most matching occurs in programs that are federally funded or controlled by Federal law. For example, States conduct matches in unemployment insurance programs to detect fraudulent and duplicative payments, and to monitor employers' contributions. Forty-one States reported conducting such matches, and 23 States reported matching unemployment insurance records with other jurisdictions.[54] Less than 20 States report matching for workers' compensation programs.[55] In public assistance programs, States generally match recipient files against quarterly wage reports submitted by employers to detect recipients who are receiving wages over an allowable limit. An OTA survey of eight States revealed that six (California, Colorado, Georgia, Illinois, Indiana, and Michigan) conducted such matches, while two States (Florida and Minnesota) did not. DEFRA now requires that this be done by all States.

Other examples of State matching activities include:

- Thirty-seven States submit social security numbers of welfare recipients to SSA for computerized verification that the numbers are accurate.
- At least two States, Massachusetts and Maryland, have authorizations in their laws for the public assistance program to conduct computer matches against the accounts of all bank customers in the State.

---

[53] Information for this section is derived from Robert Ellis Smith, *Report on Data Protection and Privacy in Seven Selected States*, OTA contractor report, February 1985.

[54] See U.S. Department of Labor Inspector General, *Inventory of Computer Matching Activities in State Labor and Related Agencies*, 1982.

[55] Ibid.

- The Immigration and Naturalization Service is encouraging States to match motor vehicle, welfare, and unemployment files with its databank of current registered aliens. Colorado, Illinois, and California have agreed. California must approve new regulations before this can be done, and the regulations have not yet been published.
- California, Minnesota, and several other States conduct Project Intercept. Lists of persons owing money to the State—either in delinquent taxes, welfare overpayments or frauds, faulty unemployment compensation, etc.—or those reported delinquent in child support payments are submitted to the public assistance agency (or any other agency making periodic payments) so that the amount owed is offset against the State payments. This is also done with tax refund checks (not only in the States, but by the IRS as well).
- Many States compare their lists of recipients, whether public assistance, unemployment compensation, or other payment programs, against comparable lists of recipients in neighboring jurisdictions, to determine who is "double-dipping." Examples are Virginia's unemployment compensation records matched with those of Maryland and the District of Columbia; or Indiana's records matched with those of Kentucky.

There are other generic exchanges of personal data by most States that are significant, although they may not be classified strictly as "matches." Many of them predate the current Federal initiative on matching, which began in 1978. They include:

- Motor vehicle departments in 49 States provide lists of young, male drivers to the Selective Service System for matching against lists of men who have registered for a military draft. Objections, based on invasion of privacy, were expressed in many States. Some laws or regulations governing DMVs seem to prohibit such disclosures. But in the end, the Selective Service System had nearly 100 percent participation.
- More than 80 percent of the motor vehicle departments disclose driving records and accident reports to Dataflo Systems, a division of Equifax, Inc., so that Dataflo can computerize the data and market it to insurance companies. The abstract includes social security number, driver's license number, birth date, physical description, restrictions on the permit, and a chronological list of violations. An insurance company can then query one of five regional computers operated by Dataflo.
- Motor vehicle departments also disclose suspended or revoked licenses to the National Driver Register operated by the U.S. Department of Transportation in Washington and, in turn, query the system when persons apply for drivers' licenses.
- Just about all motor vehicle departments rent mailing lists of licensees and of automobile owners to mailing list firms and other marketers. A report by the Secretary of State of Illinois in 1983 stated that 44 States answered in the affirmative when surveyed on whether they rent mailing lists. The other six States did not respond. Many States, however, have regulations or laws limiting, if not fully prohibiting, such disclosures.
- Every State with a State income tax has an agreement with the IRS to exchange computerized data on its taxpayers with IRS and to receive comparable information from IRS.

An analysis of State matching activities in light of State Privacy Acts or Fair Information Practices Acts indicates that the presence of such laws does not deter computer matching. However, it often assures that there is a review of a State agency's decision to match, that there are specific procedures to follow, and that information is checked for accuracy. The critical factor in determining the extent of matching at the State level appears to be the size of the population. States with larger populations engage in more computer matching than States with smaller populations.

Finding 10

All Western European countries and Canada are using computer matching or record linkages, to an increasing degree, as a technique for detecting fraud, waste, and abuse.

In general, the specific uses of matching in Western Europe and Canada are similar to those in the United States—primarily in social welfare programs.[56] In Western European countries, computer matching and other record linkage issues are handled within the context of data protection laws and oversight. In general, European data protection laws require the advice or consent of the data protection agency before any records can be linked. A brief review of matching activities in different countries follows.

Canada

The Canadian Privacy Act of 1982 does not address computer matching specifically, but does contain the principle that information should be used only for the purpose for which it was collected. The Canadian Privacy Commissioner, John W. Grace, has spoken out strongly on the privacy implications of matching. As he sees it:

> That computer-matching is carried on in the name of efficiency, good government and law enforcement makes it potentially a more, not less, dangerous instrument in the State's hands.[57]

Specific instances of matching include: opening Federal databanks to obtain information for collecting alimony and child support payments from recalcitrant fathers, Revenue Canada's matching of a provincial voters' list with tax records to identify individuals who had not filed tax returns, and matches by the Canadian Employment and Immigration Commission to detect overpayment of unemployment insurance benefits.

Sweden

Under Section 2 of the Data Act, specific permission is required from the Data Inspection Board (DIB) for the linkage of files that contain "personal data procured from any other personal file, unless the data are recorded or disseminated by virtue of a statute, a decision of the Data Inspection Board, or by permission of the person registered." DIB evaluates all proposals for record linkages and has approved an estimated 80 to 90 percent of the proposed record linkages. In reviewing proposals, DIB looks especially at the purpose of the match and the quality, e.g., timeliness, accuracy, and completeness, of the data to be used. In general, DIB is opposed to linkages of very sensitive personal information, e.g., alcoholism and drug addiction records, and linkages where the users do not know why personal information was originally collected.

DIB has not always been successful at preventing record linkages. For example, when the tax authorities sought information on income from interest and dividends from the banks, DIB said that the banks were not licensed to divulge such information to the tax authorities. Regardless, the banks gave the information to the tax authorities. DIB sought to prosecute the banks under the Data Act and the case is still under appeal.

France

The National Commission on Informatics and Freedoms (CNIL) has to authorize record linkages. In general, CNIL is opposed to linkages because of the principle that data should be used only for the purposes for which they were collected. In contrast to other countries, there are few plans for record linkages.

Federal Republic of Germany

The Republic's Federal Data Protection Act contains a general prohibition against the dissemination of personal data from one public body to another, unless the release of the information "is necessary for the legitimate accomplishment of the tasks for which the dissemination unit or the recipient is competent."

---

[56] Information for this section is derived from David H. Flaherty, "Data Protection and Privacy: Comparative Policies," OTA contractor report, January 1985.

[57] Privacy Commissioner, *Annual Report, 1983-84*, p. 3.

Computer linkages among social services occur frequently and do not have to be reported to the Data Protection Commissioners. Most linkages of social service data outside the social service administrations are prohibited by the Social Code unless the information is necessary to prevent premeditated crimes, to protect public health under certain circumstances, to implement specific stages of the taxation process, and to assist the registered alien authorities.

Finding 11

Computer matching raises a number of policy questions that warrant congressional attention, including availability of records for matching, approval before matches, notice for individuals, requirement of cost-benefit analysis, and verification of hits.

In designing policy for computer matching, consideration of the following factors is important:

Records to be made available for computer matches and for what purposes.—Currently, there are few restrictions on the systems of records that can be used. If a "routine use" can be crafted to justify the match, then almost any Federal system can be made available. The primary exception to this is IRS information, but this restriction can be circumvented somewhat by matching with a system of records that has already been matched against IRS information. Another long-standing exception has been private sector information; however, a number of new Federal and State laws now allow for such access.

In determining what records should be available, several possibilities exist. One is to make all records available for all matches. Another is to prohibit the use of some systems of records, e.g., health information, bank records, or IRS records. A third is to make the availability of records dependent on the purpose of the match. The difficulty with this alternative, which may be otherwise attractive because it allows flexibility, is that it could easily evolve into a system similar to what currently exists where routine use exceptions are not carefully scrutinized. If the use of records is to depend on the purpose of the match, then the purposes that would legitimate the use of particular systems of records need to be specifically established in advance of proposals to match.

Another issue in determining what records are to be available is the quality of records used in computer matching. Inaccurate records detract from the effectiveness of computer matching and increase the problems individuals experience as a result of a match. Record systems could be required to meet specific data quality standards prior to being used in a computer match.

Approval required before a match takes place.—Both a process for approving matches and a substantive review of the purpose of the match must be considered. In terms of process, one task is to check on and oversee program managers' decisions to match. This check could be carried out within an agency, as often appears to be the case at present, by a formal executive branch review process, or by review by a legislative body. In addition to the process, criteria need to be developed to determine the appropriateness of matching under the circumstances. Such criteria could be based on both the privacy interests involved and the management interests.

Notice to individuals.—This depends in part on the purposes of notification. Originally, notice as part of due process was viewed as a means of empowering the individual. If an individual knew what was to take place, he or she could take measures to try to stop the action. This original goal seems to have been replaced with a more passive view of notice. In part this may be attributed to the lack of options available to an individual who is dependent on government benefits or employment. If this is indeed the case, i.e., that individuals could be told of an action with no recourse, its implications need to be acknowledged.

There are limitations to the present system of placing notices in the *Federal Register*. Other alternatives include placing a notice on the original application form, having an individual sign a consent form at the time of application, writing all individuals prior to the match, and writing to obtain signed consent prior to the match.

An additional question is when to notify individuals—before they become part of the program, before the match, after matching has produced a hit, or after the hit has been verified?

Requiring cost-benefit analysis.—Originally, cost-benefit analyses were required prior to a match. Currently, cost-benefit analyses are to be filed with OMB following a match. Agencies have not welcomed the requirement of doing cost-benefit analyses. In part, this is because there are many qualitative costs that are difficult to measure. In part, it is because many of the quantitative costs are difficult to separate from other administrative costs. In determining what kind of a cost-benefit analysis to require, questions of time of submission, review, and components to be addressed need to be answered.

Verification of hits.—Other than for matches conducted under DEFRA, there are no requirements on verifying hits. Again, this involves two issues—the process of verification and the substance of what is to be verified. Specific questions include: do all hits have to be verified or only some predetermined percentage; what sources are to be used in verifying hits; if there is a discrepancy in information received, how is it resolved; and what is the role of the individual in the verification process?

Appropriate action to be taken against an individual who has submitted false information.—Presently, the individual is given an administrative hearing and can then be subject to criminal charges. If the purpose of the hearing is indeed to refine evidence for criminal proceedings, then it may be more appropriate to conduct the hearing in a formal judicial setting. Alternatively, the use of evidence from a computer match could be prohibited from criminal proceedings, allowing its use only in civil proceedings.

Chapter 4

Computer-Assisted Front-End Verification

Contents

Page
Summary 67

Introduction and Background 67

Findings 68
  Finding 1 68
  Finding 2 74
  Finding 3 78
  Finding 4 80
  Finding 5 81

Tables

Table No. *Page*
13. Computerized Databases Used for Front-End Verification 73
14. Examples of State Front-End Verification Programs 75

Figures

Figure No. *Page*
5. Current Database Linkages 69
6. Composite of Data Linkages Through Computer Matches by AFDC Programs in Various States 70
7. A Representative Income and Eligibility Verification System (IEVS) for a State Food Stamp Agency as Required by the Deficit Reduction Act of 1984 76

Chapter 4

Computer-Assisted Front-End Verification

SUMMARY

Whereas computer matching involves comparing records after an individual is already receiving government benefits or services, front-end verification is used to certify the accuracy and completeness of personal information at the time an individual applies for government benefits, employment, or services. Like computer matching, any large-scale application of front-end verification is dependent on computers and telecommunication systems.

OTA found that:

- The use of front-end verification is creating a *de facto* national database covering nearly all Americans. The technological requisites for front-end verification lead to the establishment of individual databases for verification purposes and to the connection of these databases through online telecommunication linkages.
- There is no comprehensive information on the use of front-end verification by Federal agencies. Front-end verification is used by many States, mostly in federally funded programs, and is initiated or required by the Federal Government. Legislation, either recently enacted and/or proposed, will expand the use of front-end verification at the Federal as well as the State level.
- Front-end verification raises due process and privacy issues that have not been systematically studied.
- There has been no comprehensive study of how to conduct front-end verification in the most cost-effective manner and with the highest possible data quality.
- There are no general Federal regulations, either statutory or administrative, guiding the use of front-end verification. In designing guidelines, a number of factors warrant consideration, including:
  - —the responsibility for determining access to and record quality of the databases used for verification purposes;
  - —the frequency of front-end verification, i.e., routine or selective;
  - —the rights of individuals;
  - —the types of information used; and
  - —the possible requirement of a cost-benefit analysis.

INTRODUCTION AND BACKGROUND

Computer-assisted front-end verification is used to certify the accuracy and completeness of personal information by checking it against similar information held in a computerized database, generally of a third party. It may involve certifying information that the individual has supplied, checking a database to determine if there is additional relevant information, or both. Front-end verification is used when an individual initially applies for government benefits, employment, credit, contracts, or some other government program or service. In the past, such verification was done manually on a random basis or when the accuracy of information provided was suspect. Today, the number of applications and details to be verified makes manual verification prohibitive in terms of cost and time; however, computerized databases and on-line networking make it possible to carry out such verification routinely.

Front-end verification is similar to computer matching in that it involves an electronic search for the purpose of ensuring the accuracy and completeness of information to maintain the integrity of government programs. However, front-end verification differs from computer matching in four ways: 1) information is verified on an individual basis, rather than for a category or class of people; 2) information is verified before an individual receives any government benefits or employment; 3) its purpose is to prevent and deter, rather than to detect and punish; and 4) it is done most effectively at the time of the initial transaction, and thus accelerates the trend to on-line data linkages. For these reasons, some of the policy issues (e.g., data quality, cost-effectiveness, and administrative discretion) are essentially the same for both front-end verification and computer matching. However, other issues, such as due process and privacy concerns, are different for front-end verification than for matching.

Computer-assisted front-end verification can be done in two ways—by batch processing or by a direct on-line inquiry. If batch processing is used, the agency compiles (usually on magnetic tape) all information needing a specific type of verification, either at the end of the day or week, and sends it to the relevant source for verification. A tape-to-tape match reveals inconsistencies in the data. The second method is a direct on-line inquiry from an agency terminal to the computerized source database as each individual case is considered. An immediate on-line response reveals inconsistencies in the data. Because of its speed and efficiency, the trend is toward more direct on-line verification. For example, the Department of Health and Human Services found that 73 percent of front-end verification in the Aid to Families With Dependent Children (AFDC), food stamp, and Medicaid programs at the State level was conducted on-line.[1]

FINDINGS

Finding 1

The use of front-end verification is creating a *de facto* national database covering nearly all Americans. The technological requisites for front-end verification lead to the establishment of individual databases for verification purposes and to the connection of these databases through on-line telecommunication linkages.

This *de facto* national database is not a centralized database in the sense that all information is contained in one mainframe computer housed in one building. Instead, the present dominant approach is to create a "virtual" central databank by electronically (via direct online linkages[2] or exchange of computer tapes) combining and comparing information from several separate, usually remote, record systems. If enough separate record systems are queried, the result can be the creation of a *de facto* electronic dossier on specific individuals. See figures 5 and 6 for attempts to portray the current state of computerized linkages among separate databases.

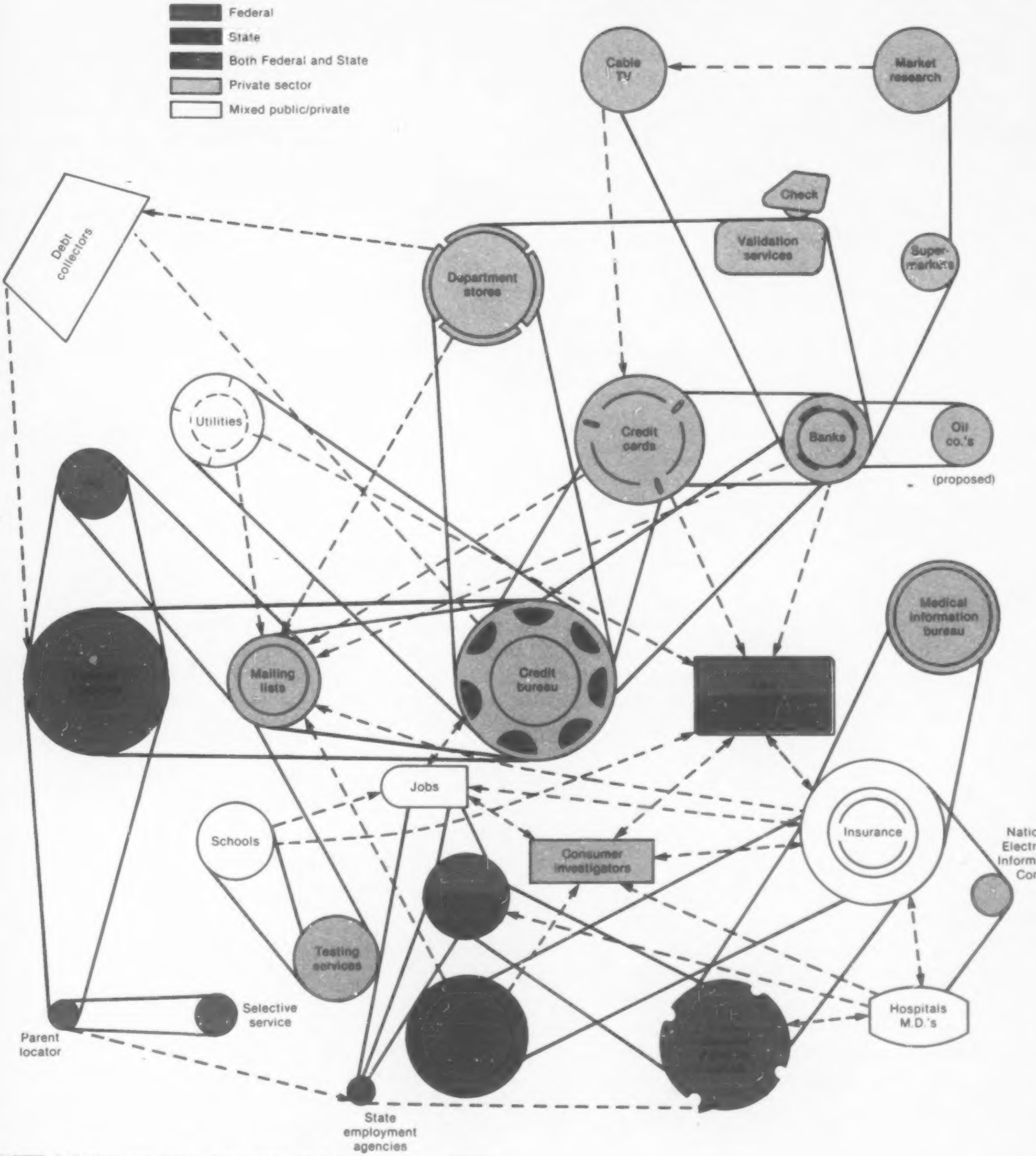
Part of the explanation for this decentralized approach to databanks and dossiers, rather than a centralized approach, is that advances in computer and data communication technology have reduced the technical and cost barriers to such interconnections. However, part of the explanation is also political in nature. The decentralized approach reflects the fragmented and complex structure of the executive branch of the Federal Government. Although Federal agencies may collect and use similar information on individuals, they also collect information that is specific to their missions and would prefer to maintain their own

---

[1] U.S. Department of Health and Human Services, Office of Inspector General, *Catalog of Automated Front-End Eligibility Verification Techniques: A Project of the President's Council on Integrity and Efficiency*, OAI-85-H-51, September 1985, p. 13.

[2] On-line telecommunication linkages involve data communications, the contents of which are not protected by existing statutory (e.g., Title III of the Omnibus Crime Control and Safe Streets Act) and constitutional prohibitions on the interception of phone calls. See U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985).

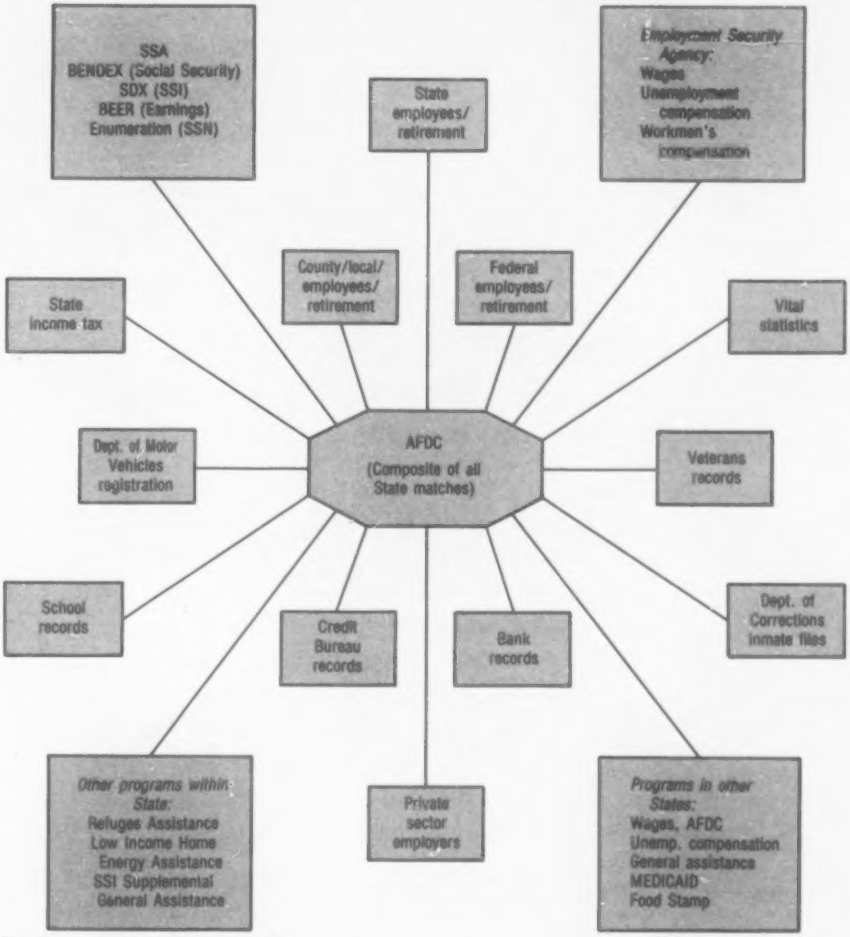
Figure 5.—Current Database Linkages



NOTES: Solid lines—automated exchanges; dotted lines—manual exchanges.

SOURCE: *The Privacy Journal*, April 1984, p. 5.

Figure 6.—Composite of Data Linkages Through Computer Matches by AFDC[a] Programs in Various States


SSA
BENDEX (Social Security)
SDX (SSI)
BEER (Earnings)
Enumeration (SSN)
State employees/ retirement
Employment Security Agency:
Wages
Unemployment compensation
Workmen's compensation
County/local/ employees/ retirement
Federal employees/ retirement
State income tax
Vital statistics
Dept. of Motor Vehicles registration
AFDC (Composite of all State matches)
Veterans records
School records
Credit Bureau records
Bank records
Dept. of Corrections inmate files
Other programs within State:
Refugee Assistance
Low Income Home Energy Assistance
SSI Supplemental
General Assistance
Private sector employers
Programs in other States:
Wages, AFDC
Unemp. compensation
General assistance
MEDICAID
Food Stamp

[a] Aid to Families With Dependent Children.

NOTE: No single State has all of these links, but each link occurs in at least one State. With a few exceptions, however, these types of sources could be available in every State.

SOURCE: U.S. Department of Health and Human Services, Office of Inspector General, Inventory of State Computer Matching Technology, and GAO observation.

databases for their clients or employees. Additionally, the decentralized approach reflects incremental responses to policy problems. Databases usually are created to deal with a specific problem as seen at a particular time. Rarely is the opportunity taken to review related problems and look for a common solution.

The decentralized approach also reflects political concerns frequently expressed about centralized databanks and dossiers. Indeed, when proposals for various national databanks were first made 15 to 20 years ago, the reaction was quite negative. Concern was expressed that, even if central databanks were technically feasible, they might be more open to abuse, and might consolidate power and control in the Federal Government.[3] Since that time, few proposals for national databanks of personal information have been made or seriously considered. In cases where there has been a serious debate, the common result has been a decentralized approach. Two cases in point are the Interstate Identification Index (known as Triple I), run by the Federal Bureau of Investigation (FBI), and the National Drivers Register (NDR) run by the Department of Transportation's National Highway Traffic Safety Administration (NHTSA).

In both of these situations, proposals to maintain central databanks (on criminal history records and motor vehicle operator records, respectively) run by the Federal Government were strongly opposed by various States and civil liberty groups and ultimately defeated, even after partial implementation. In both cases, a decentralized index approach was adopted (with support from the States and civil liberty groups) as an alternative to the central databank approach. In the index approach, the Federal Government (in these examples, the FBI and NHTSA) maintains, in effect, an index to records in State record systems. Only names and identifiers are contained in the index—it does not include information about specific offenses, charges, and dispositions (for criminal history records indexed by the Triple I) or about specific driver violations and license suspensions (for vehicle operator records indexed by NDR).

The NDR contains 10 million records with information on drivers' licenses that have been revoked or suspended in various States. NDR is a voluntary Federal/State cooperative program to aid States in exchanging information about the driving records of certain individuals. Currently all States participate in reporting license withdrawals, submitting names to be checked against the NDR file, or both. NDR has been in operation since 1961 under the authority of Public Law 86-660, which directed the Secretary of Commerce to establish a register of all names of individuals reported by the States for revocation of a driver's license because of driving while intoxicated or violation of a highway safety code involving loss of life. Until 1982, reports on license withdrawals and denials contained descriptive information about the individual and details of the adverse action taken. The National Drivers Register Act of 1982 (Public Law 97-364) requires that the content of the Federal NDR file be limited to minimal, personal, identifying information with case-specific information being maintained only by the State instituting the adverse action. The 1982 law also converted NDR to a fully automated system.

The FBI's Triple I, which became operational on February 7, 1983, contained 9,268,332 records as of May 1, 1985.[4] Triple I is essentially an index of persons with criminal history records on file at the FBI and/or in State criminal history record repositories. For each person listed, Triple I includes only information on personal descriptors, identifying numbers, and the location(s) of the criminal history record(s). At present, use of Triple I is limited to criminal justice and criminal justice employment purposes, although the question of noncriminal justice use (primarily for employment and licensing checks) has not been resolved (see app. A at the end of this report for further discussion). If authorized criminal justice agencies obtain a "hit" or match on Triple I, the agencies obtain the actual criminal history record information from the FBI (for Federal offenders and offenders from States not yet participating in Triple I) or from State criminal record repositories (for Triple I participants). Triple I inquiries are made electronically via the National Crime Information Center's (NCIC) communication lines and, if a hit occurs, are referred or switched automatically to the appropriate holder of the original criminal history record. Records are provided by one or a combination of the following: on-line via NCIC, electronically from a State via the National Law Enforcement Telecommunications System, or by mail from the FBI or State repository.

---

[3] See U.S. Congress, House Committee on Government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and Invasion of Privacy*, hearings, 89th Cong., 2d sess., July 25, 27, 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966); and U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasion of Privacy*, hearings, 89th Cong., February 1965 to June 1966 (Washington, DC: U.S. Government Printing Office, 1965-67).

[4] FBI response to OTA Federal Agency Data Request. Also see U.S. Department of Justice, Federal Bureau of Investigation, Technical Services Division, *Statement of Work for NCIC 2000 (2K) Project—PHASE I: A Comprehensive Study To Define: System Requirements, Functional Design and System Specs (Consistent With a Rigorous Environmental Analysis/Evaluation)*, January 1985, p. A9; and David F. Nemecek, "The Interstate Identification Index (III)," *Interface*, SEARCH Group, Inc., vol. 9, No. 1, summer 1984, pp. 10-11.

Triple I represents an alternative to the now-defunct Computerized Criminal History (CCH) file previously maintained in NCIC. By including index entries for computerized criminal history records maintained by the FBI's Identification Division, as well as records from participating States, Triple I has been able to facilitate access to and exchange of over 9 million criminal history records, compared to the roughly 2 million records contained in the old NCIC/CCH file. However, there still are several unresolved issues concerning Triple I—noncriminal justice use, record quality, and policy oversight. These are discussed in further detail in appendix A to this report.

The decentralized approach in these instances is generally perceived as minimizing adverse impacts on Federal-State relations, since the States retain primary control over the source records. Also, the risk of abuse or misuse by the Federal Government is thought to be lessened, since there is no central file. However, authorized Federal, State, and local agencies can determine, via the index, the location of records of interest and request such records directly from the State record repositories. Thus, a dossier on any given individual can be compiled by consolidating various records from separate State agencies. It is also possible for Federal agencies to run a longer list of persons against the index to see if there are any matches, or "hits," and then follow up to obtain more detailed information.

Agencies may also maintain a centralized index of individuals whose records are maintained in their computerized databases. For example, the OTA survey revealed that the Immigration and Naturalization Service (INS) has a Central Index System (CIS) of 152 million records that contains file location, immigration status, and biographical data on individuals of interest to INS. On-line access to CIS is provided at ports of entry, file control offices, border patrol headquarters, and other agencies involved in intelligence or law enforcement. On an average, 600 users generate 100,000 file accesses per day.

Although electronically linked, on-line databases are distributed in a physical sense, they constitute a centralized database in a practical sense. As more and more systems automate and have on-line communication capability, this virtual database will grow. There are a number of computerized databases that are accessible by selected government agencies for computer-assisted verifications—for example, the computer files of the FBI's NCIC and those of the Bureau of the Customs' Treasury Enforcement Communication System. INS maintains a number of computerized record systems —the Anti-Smuggling Information System, the Central Index System, the Non-Immigrant Information System, the Student School System, and the National Automated Immigration Lookout System. The Social Security Administration (SSA) also maintains a number of databases for verification purposes—the State Data Exchange, the Beneficiary and Earnings Data Exchange, the Third Party Query, and the Enumeration Search and Verification Response System. Additionally, private sector firms, such as credit bureaus and medical insurers, maintain a number of centralized databases that are accessible by government agencies. See table 13 for a description of these databases.

Centralized databases are also created from existing decentralized databases. One example is the IRS's Debtor Master File, which was

Table 13.—Computerized Databases Used for Front-End Verification

National Crime Information Center (NCIC).—There are 12 files containing a total of 16,395,662 files (as of 5/1/85) that can be accessed through the NCIC system.[a] The 12 files include: the Interstate Identification Index (III) File, the Stolen Securities File, the Stolen Guns File, the Stolen Articles File, the Stolen Vehicles File, the Stolen License Plates File, the Wanted Persons File, the Missing Persons File, the Stolen Boats File, the Canadian Warrant File, the U.S. Secret Service Protective File, and the Unidentified Persons File. NCIC functions as a nationwide computerized information service for Federal, State, and local criminal justice agencies.

Treasury Enforcement Communication System (TECS).—Includes a range of information on persons suspected of, or wanted for, violations of U.S. Customs or related laws—e.g., persons suspected of or wanted for thefts from international commerce, and persons with outstanding Federal or State warrants. The Border Enforcement System is the major component and is used to: assist Customs and the Immigration and Naturalization Service (INS) personnel screen persons and property entering and exiting the United States; provide investigative data to Customs or other agency law enforcement or intelligence officers; and aid in the exchange of data with other Federal, State, or local law enforcement agencies. As of May 1, 1985, the Border Enforcement System included computerized records on over 2 million persons.

Nonimmigrant Information System (NIIS).—Contains over 32 million records on foreign visitors, diplomats, and students for purposes of tracking their movements. The system has been operational since January 1983. The student/schools subsystem became operational in August 1984 and tracks 500,000 students at 15,000 schools.

Anti-Smuggling Information System (ASIS).—Incorporates 750,000 records containing information relating to alien smugglers, including names (and aliases), addresses, phone numbers, and license plates.

National Automated Immigration Lookout System (NAILS).—Provides on-line information for the detection of inadmissible persons and others of particular interest to INS and other law enforcement agencies. Presently contains 40,000 records.

State Data Exchange (SDX—Social Security Administration [SSA]).—Contains 7.5 million records with title XVI information extracted from the supplemental security record, as well as Medicaid eligibility data for specified States. SDX has been in operation since December 1973 and is accessible by State Welfare/Human Resources Departments for use in administration of income maintenance and Medicaid programs.

Beneficiary and Earnings Data Exchange (BENDEX—SSA).—Contains 64 million records with information on title II eligibility, Medicare entitlement, wage data, and eligibility entitlement to other SSA-administered programs. BENDEX has been in operation since 1968 and is accessible by State Welfare/Human Resources Departments for use in administration of income maintenance programs.

Third Party Query (TPQY—SSA).—Contains the 7.5 million SDX records and the 64 million BENDEX records. TPQY has been in operation since November 1984 and is accessible for purposes of speeding up the SSA-administered benefit verification process by all State, local, and Federal agencies that administer a health and/or income maintenance program (including commercial vendors).

Enumeration Search Verification and Response System (ESVARS—SSA).—Contains identification data for every social security number that has been issued. There are 280 million base records, which are expanded to 420 million iterations because of name changes, duplicate cards, and such. ESVARS has been in operation since Apr. 1, 1985 and is accessible by all SSA employees who need to verify social security numbers and Federal, State, local, and private agencies that justify their need to verify social security numbers.

[a]For further discussion, see app. A at the end of this report. Also see U.S. Congress, Office of Technology Assessment, *An Assessment of Alternatives for a National Computerized Criminal History System*, OTA-CIT-161 (Springfield, VA: National Technical Information Service, October 1982).

SOURCE: Office of Technology Assessment.

created in 1986 using information from the databases of a number of agencies. The Debtor Master File was authorized in the Deficit Reduction Act. The purpose of the Debtor Master File is to aid in administering the offset of tax refunds to collect on delinquent Federal debts, such as student loans.[5] The 1986 Debtor Master File contains the names of 750,000 individuals who are indebted to at least one of the following agencies: the Departments of Education, Housing and Urban Development, or Agriculture; the Veterans Administration; and the Small Business Administration. Preoffset notices were sent to these individuals and resulted in payments from 41,000 persons totaling $14 million.[6]

As the exchange of information becomes faster and easier, there will be pressure to increase computer connections and on-line processing. The Deficit Reduction Act and the establishment of Income Eligibility Verification Systems (IEVS) is a good example (see app. E of this report). Under the rules issued by the Departments of Labor, Agriculture, and Health and Human Services,[7] IEVS would contain wage and benefit data from State Wage Information Collection Agencies; wage, benefit, and other income data from SSA; and unearned income data from the Internal Revenue Service (IRS). The Deficit Reduction Act requires each State to establish an Income Eligibility Verification System. The rules do not interpret this as mandating a physical system, but a logical process that would assure timely and efficient exchange of data. Compatibility to allow exchanges of data among various IEVS is a possibility. The Deficit Reduction Act also requires each State to collect quarterly wage reports from all employers and to establish a State Wage Information Collection Agency that will maintain records of social security numbers; full name; quarterly wages; and employer's name, address, and identifier. As of 1982, 12 States did not collect wage information on a quarterly basis.[8]

---

[5] U.S. Department of the Treasury, Internal Revenue Service, "Privacy Act of 1974; System of Records," *Federal Register*, vol. 50, No. 195, Oct. 8, 1985, p. 41085.

[6] See David Burnham, "I.R.S. To Withhold Tax Refunds Owed Loan Defaulters," *New York Times*, Jan. 10, 1986, pp. A1, A11; Keith B. Richburg, "Agencies Give Defaulters' Names to IRS," *Washington Post*, Jan. 10, 1986, p. A21; and Judith A. Sullivan, "IRS To Collect Agencies' Debts," *Government Computer News*, Sept. 13, 1985, pp. 1, 16.

The result of IEVS will be uniformity among State systems. The Department of Agriculture has agreed that State Wage Information Collection Agencies should collect the following information: social security number; full name; quarterly wages; and employer's name, address, and identifier. Additionally, the need to follow specific guidelines in accessing IRS and SSA information will also create more uniform systems throughout the States, and is tantamount to the establishment of a *de facto* wage and eligibility recipient system. In the congressional debates on the Deficit Reduction Act there was no explicit discussion of such a system.

Finding 2

There is no comprehensive information on the use of front-end verification by Federal agencies, although the Federal Government is increasingly requiring front-end verification in many federally funded programs administered by the States. Recently enacted legislation will expand the use of front-end verification at the Federal as well as the State level.

Because the personal information provided by applicants for government programs is often inaccurate or incomplete, front-end verification is useful for checking eligibility for Federal benefit programs, checking on current debts and earnings for loan applicants, and checking financial and criminal histories for employment applicants.

The existence of the numerous computerized databases discussed above would seem to indicate that many agencies use front-end verification. However, only two agencies—the Bureau of Indian Affairs in the Department of the Interior and the Veterans Administration—responded affirmatively to the OTA survey's question on front-end verification. In part, the small number of affirmative responses to the question may be attributed to a lack of understanding of what would be termed "front-end verification."

Until recently, there was almost no information on State use of front-end verification. However, the Department of Health and Human Services has recently completed a survey of automated front-end eligibility verification applications currently used or being developed at the State level for use in AFDC, food stamp, Medicaid, and unemployment insurance programs. With a 92 percent response rate from the States, the survey found 75 front-end verification applications being used in AFDC, food stamp, and Medicaid programs in 36 States, and 53 front-end verification applications being used in unemployment insurance programs in 36 States.[9] The primary data checked in these front-end verifications include duplicate benefits, earned income, and work history. Examples of some front-end verification programs appear in table 14.

---

[7] Departments of Labor, Agriculture, and Health and Human Services, "Income & Eligibility Verification Procedures for Food Stamps, Aid to Families With Dependent Children, State Administered Adult Assistance, Medicaid and Unemployment Compensation Programs: Final Rule," *Federal Register*, vol. 51, No. 40, Feb. 28, 1986, pp. 7178-7217.

[8] U.S. Congress, Hearings Before the Senate Committee on Governmental Affairs, Subcommittee on Oversight of Government Management, *Oversight of Computer Matching To Detect Fraud and Mismanagement in Government Programs*, Dec. 15-16, 1982 (Washington, DC: U.S. Government Printing Office, 1982), p. 14.

There has been a marked increase in State use of front-end verification in Federal welfare programs. Federal statutes, most notably the Deficit Reduction Act, now require front-end verification in certain programs. The Deficit Reduction Act requires States to use front-end verification in administering the food stamp, AFDC, unemployment compensation, Medicaid, and SSA's adult assistance programs (titles I, X, XIV, XVI). The sources that will be used most frequently for verifying information are: the agency's own data sources, as a check on duplicate benefits; SSA's State Data Exchange System (SDX), which contains a listing of all supplemental security income recipients in the State; the SSA's Beneficiary and Earnings Data Exchange (BENDEX), which contains wage data and eligibility entitlements to SSA programs; SSA's Enumeration Verification System (EVS), which contains information on social security numbers; IRS files for earned and unearned income; INS files for immigration status; and State wage data systems (see fig. 7).

Under the rules developed by the Departments of Labor, Agriculture, and Health and Human Services, States are required to develop a statewide IEVS, and to use SSA and IRS systems for verifying additional information. Examples of front-end verification required under the Deficit Reduction Act include verification of: social security numbers through BENDEX, SDX, or EVS; unearned income through IRS with subsequent verification from the individual or source of unearned income; and income/wages through IEVS.[10]

Table 14.—Examples of State Front-End Verification Programs

Nevada.—The Welfare Referral System under development will provide the caseworker with information about the applicant's receipt of income assistance benefits, wages, and unemployment compensation benefits (UCB). When an applicant comes into the local office, the worker will enter the applicant's name, social security number, and other data into the "key file." This information will be matched on-line against welfare and wage and UCB data (welfare refers to Aid to Families With Dependent Children (AFDC), food stamps, Medicaid, child support, and social services). A hardcopy of the match will be generated and transmitted to the worker.

Georgia.—At the time of application, the eligibility worker does an on-line check of the current recipient database to detect any duplicate benefits. In addition, this match is also run during the batch processing of the application that occurs immediately prior to payment. Results are received prior to eligibility certification. This batch match also accesses statewide records of closed benefit cases. The duplicate benefit check is part of Georgia's larger Public Assistance Reporting System (PARIS) designed to collect, store, and generate information utilized by the AFDC, food stamp, and Medicaid programs.

New York.—As a new subsystem of the Welfare Management System, the Resource File Integration automatically provides front-end matching of all applicants for public assistance against the State wage file. The wage data is available on-line to eligibility workers. To assure that local workers take action on the information, a resolution code indicating the action is required before any further processing can take place. Future plans call for adding State UCB data to the resource file. This system is used statewide except in New York City, which has a slightly different system providing the same information by overnight batch processing.

Florida.—Information on individuals who are known to have been involved in labor disputes and who have committed benefit fraud is stored in the claim history file. When an individual applies for unemployment compensation benefits, employees automatically perform an on-line match between this data and applicant data when they enter data from a new application. Positive hits generate flags that prevent any payments from being made until the issue is resolved.

SOURCE: U.S. Department of Health and Human Services, Office of Inspector General, *Catalog of Automated Front-End Eligibility Verification Techniques*, OAI-85-H-51, September 1985.

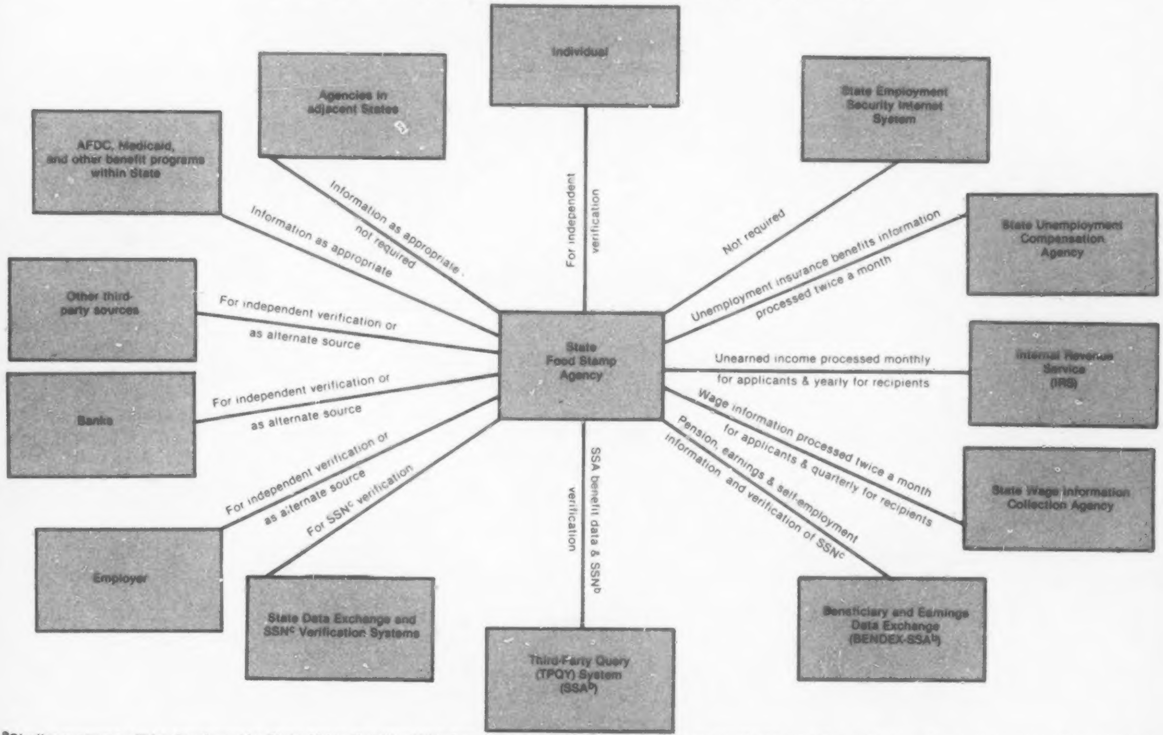
The Debt Collection Act requires applicants for Federal loans to supply their taxpayer identification number (for individuals, their social security numbers), and requires agencies to screen credit applicants against IRS files to check for tax delinquency. Circular A-70 of the Office of Management and Budget (OMB)

---

[9] U.S. Department of Health and Human Services, *Catalog of Automated Front-End Eligibility Verification Techniques*, op. cit.

[10] See app. E of this report.

Figure 7.—A Representative Income and Eligibility Verification System (IEVS) for a State Food Stamp Agency as Required by the Deficit Reduction Act of 1984[a]


Individual
For independent verification
Agencies in adjacent States
Information as appropriate, not required
AFDC, Medicaid, and other benefit programs within State
Information as appropriate
Other third-party sources
For independent verification or as alternate source
Banks
For independent verification or as alternate source
Employer
For independent verification or as alternate source
State Data Exchange and SSN[c] Verification Systems
For SSN[c] verification
Third-Party Query (TPQY) System (SSA[b])
SSA benefit data & SSN[b] verification
State Food Stamp Agency
State Employment Security Internet System
Not required
State Unemployment Compensation Agency
Unemployment insurance benefits information processed twice a month
Internal Revenue Service (IRS)
Unearned income processed monthly for applicants & yearly for recipients
State Wage Information Collection Agency
Wage information processed twice a month for applicants & quarterly for recipients
Beneficiary and Earnings Data Exchange (BENDEX-SSA[b])
Pension, earnings & self-employment information and verification of SSN[c]

[a]Similar systems will be developed by State Aid to Families With Dependent Children (AFDC) agencies, Medicaid agencies, and unemployment compensation agencies, as well as for the Adult Assistance Program in the Territories.
[b]Social Security Administration.
[c]Social security number.

SOURCE: Office of Technology Assessment.

mandates that Federal agencies must conduct a credit screen on a potential candidate before issuing a contract, grant, loan, or loan guarantee.

With debt collection and with credit screening, the Federal Government is relying on private sector databases for verifying the information. As presently planned, five companies, including TRW Information Services, will develop databanks on individuals' credit and debt information from private and governmental sources, and two companies, TRW and Dun & Bradstreet, will do likewise for commercial firms.[11] Dun & Bradstreet's Director of Corporate Government Services was quoted as saying:

> Private lenders, banks, etc., who are Dun & Bradstreet subscribers can get this data, too. So, if you don't pay the Feds, from now on it'll affect your commercial credit rating, too.[12]

There has also been an increased effort to require criminal history record checks for job applicants in sensitive categories, e.g., day-care providers for children. Congress included a provision in the Continuing Appropriation Act of 1985 (Public Law 98-473) requiring that States establish procedures to provide for nationwide criminal history checks for all operators and employees of child-care facilities.[13] States were to have such procedures in place by September 30, 1985.[14] According to the Office of the Inspector General, U.S. Department of Health and Human Services, as of November 1984, 3 States (California, Georgia, Minnesota) had statutes requiring FBI criminal record checks on day-care providers, 24 States conducted statewide criminal record checks on day-care providers, and 20 States were anticipating new legislation authorizing such criminal record checks.[15] There has also been growing interest in implementing criminal record checks for teachers, youth group leaders, and elder-care providers.[16]

---

[11] "Front-End Credit Screening: How an Ounce of Prevention Could Avoid Billions in Cure," *Government Executive*, January 1985, pp. 34-35.

[12] Ibid, p. 35.

IRS files are also considered to be valuable sources of information for many record linkages because of the variety of information on file (e.g., address, earned income, unearned income, social security number, and number of dependents) and because the information is relatively up to date. As a general rule, returns and return information are to remain confidential, as provided for in Section 6103 of the Tax Reform Act of 1976. Under this section, information may be disclosed for tax and audit purposes and proceedings, and for use in criminal investigations if certain procedural safeguards are met.

Additionally, Section 6103(l) allows for the disclosure of return information for purposes other than tax administration. The list has grown considerably since 1976, and includes disclosures to: SSA and the Railroad Retirement Board (Public Law 94-455, 1976); Federal loan agencies regarding tax delinquent accounts (Public Law 97-365, 1982); the Department of Treasury for use in personnel or claimant representative matters (Public Law 98-369, 1984); Federal, State, and local child support enforcement agencies (Public Law 94-455, 1976); and Federal, State, and local agencies administering certain programs under the Social Security Act or Food Stamp Act of 1977 (Public Law 98-369, 1984). Section 2651 of the Deficit Reduction Act also amends Section 6103(l) of the Tax Reform Act and allows return information from W-2s and unearned income reported on 1099s to be divulged to any Federal, State, or local agency administering one of the following programs: AFDC; medical assistance; supplemental security income; unemployment compensation; food stamps; State-administered supplementary payments; and any benefit provided under a State plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Section 6103(m) of the Tax Reform Act also provides for disclosure of taxpayer identity information to a number of agencies, including the National Institute for Occupational Safety and Health and the Secretary of Education.

Pressure to extend the list of agencies that can access IRS information has intensified with interest in record linkages to detect fraud, waste, and abuse; to register men for the Selective Service; and for any program that needs a current address for an individual. The IRS's position is that its goal is to maintain a voluntary tax system and that public perception that tax information be confidential is important to maintaining a voluntary system. Thus, the IRS is, in principle, opposed to disclosing tax information.

The potential for expanding the use of front-end verification for government programs, loans, and employment is enormous, as evidenced by the Reagan Administration's proposed Payment Integrity Act that would require front-end verification in 12 new programs, including Pell Grants, guaranteed student loans, school lunches, health education loans, veterans' programs, Department of Housing and Urban Development housing programs, and railroad retirement. Additionally, the Administration would expand the types of data available for verification beyond those specified in the Deficit Reduction Act to include alien status, government wages and pensions, veterans' benefits, and railroad retirement.

---

[13] U.S. Department of Health and Human Services, *Model Child Care Standards Act—Guidance to States To Prevent Child Abuse in Day Care Facilities*, Washington, DC, January 1985, p. 2.

[14] Ibid., p. 3.

[15] Ibid., p. 27.

[16] See, for example, Adrian Higgins, "Day Care Worker Checks Getting Mixed Reviews, *Arlington Journal*, Sept. 6, 1985, p. A7; Linda Lantor, "Fairfax Schools To Tighten Employee Screening," *Arlington Journal*, Sept. 10, 1985; p. A4; and Andee Hochman, "Youth Workers Face Additional Screening; Change Follows Spate of Sex Abuse Cases, *The Washington Post*, Sept. 23, 1985, pp. D1-D2.

Another section of the proposed Payment Integrity Act would set up a Health Insurance Verification System that would enable federally funded health care programs to access third-party insurance files to verify information supplied by the person applying for insurance payments. The Federal programs include Medicaid, Medicare, Veterans, Indian Health, Black Lung, and Maternal and Child Health. The third-party insurance files to be accessed include private insurance companies, health maintenance organizations, self-insured employer-based plans, State and local employee health plans, Federal health insurance programs, and Federal and State workers' compensation.

There are presently a number of front-end verification pilot projects being conducted at the Federal level or at the State level with Federal funds. One is the Systematic Alien Verification for Entitlements (SAVE) system operated by the Immigration and Naturalization Service. State welfare agencies can access SAVE to determine if an applicant is a legal alien. Such information was previously verified by sending individual forms to INS. SAVE in this way saves time for the applicant, although State laws generally require welfare agencies to act on an application within 10 days. However, INS also regards it as a "policing tool," as indicated by this statement in an INS memo about SAVE:

> Success will be measured by the number of criminal prosecutions resulting from these efforts; the dollars of cost avoidance; and the number of unentitled aliens identified and removed or barred from benefit rolls.[17]

Another pilot project is Project Checkmate in the District of Columbia. In this project, AFDC applicants are screened against credit bureau records providing information on income, resources, bank accounts, credit balances, and employment.[18]

Finding 3

Front-end verification raises due process and privacy issues that have not been systematically studied.

Under traditional due process principles, it is arguable that individuals should be notified that information they provide will be verified by third-party sources.[19] In many of the front-end verification programs currently being used, individuals are not informed or are only informed indirectly, i.e., they are told that information may be verified, but not when or how. They are often left with the impression that they will be responsible for bringing proof to verify information, not that the agency will verify information from other sources (see box B).

The Deficit Reduction Act and the Debt Collection Act include requirements that agencies give some notice to individuals. The Deficit Reduction Act requires agencies to notify applicants at the time of application and periodically thereafter that information about them will be exchanged and used to verify income and eligibility. Under the proposed rules, it is not clear how this will be done ("in writing at application, but not necessarily on the application form") or how specific will be the information that is provided to the individual.

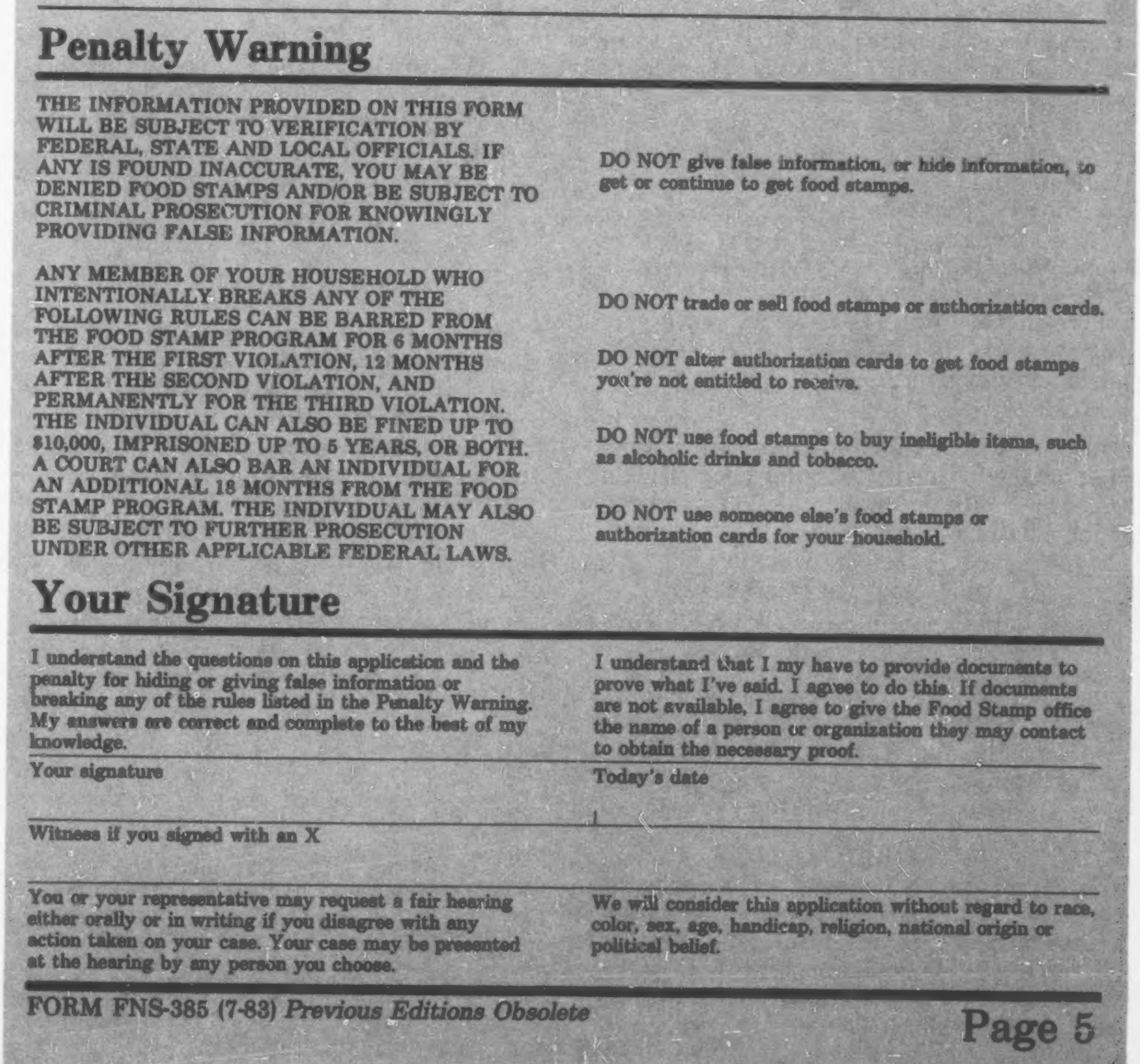
---

[17] As quoted in American Civil Liberties Union, "Computer Matching—Focus Paper," September 1985, p. 5.

[18] U.S. Department of Health and Human Services, *Catalog of Automated Front-End Eligibility Verification Techniques,* op. cit., p. 44.

[19] Procedural due process traditionally means that an official government action must meet certain standards of fairness to an individual. This generally includes the rights of adequate notice and of a meaningful opportunity to be heard prior to a decision. In determining the level of procedural due process that is appropriate, three issues are considered: 1) is there a threat to life, liberty, or property interests; 2) what are the interests of the government and of the individual; and 3) what procedures are cost-justified. See Kenneth C. Davis, *Administrative Law Treatise,* 2d ed. (San Diego, CA: K.C. Davis Publishing, 1979); Kenneth C. Davis, *Discretionary Justice: A Preliminary Inquiry* (Urbana: University of Illinois Press, 1969); and Ernest Gellhorn and Barry B. Boyer, *Administrative Law and Process* (St. Paul, MN: West Publishing, 1981).

Box B.—Example of Front-End Verification Notice



Penalty Warning

THE INFORMATION PROVIDED ON THIS FORM WILL BE SUBJECT TO VERIFICATION BY FEDERAL, STATE AND LOCAL OFFICIALS. IF ANY IS FOUND INACCURATE, YOU MAY BE DENIED FOOD STAMPS AND/OR BE SUBJECT TO CRIMINAL PROSECUTION FOR KNOWINGLY PROVIDING FALSE INFORMATION.

ANY MEMBER OF YOUR HOUSEHOLD WHO INTENTIONALLY BREAKS ANY OF THE FOLLOWING RULES CAN BE BARRED FROM THE FOOD STAMP PROGRAM FOR 6 MONTHS AFTER THE FIRST VIOLATION, 12 MONTHS AFTER THE SECOND VIOLATION, AND PERMANENTLY FOR THE THIRD VIOLATION. THE INDIVIDUAL CAN ALSO BE FINED UP TO $10,000, IMPRISONED UP TO 5 YEARS, OR BOTH. A COURT CAN ALSO BAR AN INDIVIDUAL FOR AN ADDITIONAL 18 MONTHS FROM THE FOOD STAMP PROGRAM. THE INDIVIDUAL MAY ALSO BE SUBJECT TO FURTHER PROSECUTION UNDER OTHER APPLICABLE FEDERAL LAWS.

DO NOT give false information, or hide information, to get or continue to get food stamps.

DO NOT trade or sell food stamps or authorization cards.

DO NOT alter authorization cards to get food stamps you're not entitled to receive.

DO NOT use food stamps to buy ineligible items, such as alcoholic drinks and tobacco.

DO NOT use someone else's food stamps or authorization cards for your household.

Your Signature

I understand the questions on this application and the penalty for hiding or giving false information or breaking any of the rules listed in the Penalty Warning. My answers are correct and complete to the best of my knowledge.

I understand that I my have to provide documents to prove what I've said. I agree to do this. If documents are not available, I agree to give the Food Stamp office the name of a person or organization they may contact to obtain the necessary proof.

Your signature	Today's date
Witness if you signed with an X	

You or your representative may request a fair hearing either orally or in writing if you disagree with any action taken on your case. Your case may be presented at the hearing by any person you choose.

We will consider this application without regard to race, color, sex, age, handicap, religion, national origin or political belief.

FORM FNS-385 (7-83) *Previous Editions Obsolete*

Page 5

From prototype of food stamp application approved by the Office of Management and Budget. Actual forms vary by State.

In 1983, OMB issued its *Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974.*[20] The guidelines specify that before an agency discloses information to a consumer reporting agency, the agency head or designee must review and validate the disclosure, must have given notice to the debtor of the overdue debt and its intention to disclose, must have given the individual time to file for review, and must have published a notice in the *Federal Register* identifying those systems of records from which they intend to disclose. Disclosure should be limited to that information directly related to the identity of the debtor and the history of the claim. Although under the act the consumer reporting agencies receiving records are exempt from criminal liability for misuse of information, the guidelines indicate that it would be appropriate to incorporate assurances to this effect in service contracts between Federal and consumer reporting agencies. The guidelines also clarify that nothing in the wording of the Debt Collection Act authorizes agencies to share information among themselves or to use information obtained under this act for any other purpose.

---

[20] Apr. 11, 1983 (effective Mar. 30, 1982) (43 FR 15556).

In general, it can be a simple process to notify applicants that information they provide will be verified before benefits are granted and which databases will be searched for verification of which data elements. Some even envision verification being completed while the individual waits. However, there is some question whether notice is useful for the individual under these circumstances. The purpose of notice is to give the individual information so he or she can act.[21] In the case of front-end verification, notice generally leaves the individual only one recourse if he or she does not want the information verified, and that is to withdraw the application.

The exchanges of personal information necessitated by front-end verification may conflict with the Privacy Act principles that information should be collected directly from the individual and that information collected for one purpose should not be used for another purpose without the consent of the individual. Although in front-end verification information may originally be collected directly from the individual, additional information is provided from outside sources. Moreover, the information being used to verify information provided by the individual is being used for a purpose other than that for which it was originally collected.

With respect to access to IRS information, Sections 6103(l) and (m) of the IRS code specify procedures that parties are to follow. Moreover, Federal, State, and local employees outside of IRS who handle IRS information are subject to the same criminal liabilities as IRS employees for misuse or disclosure of the information. The IRS also puts out a publication, *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Publication 1075; Rev. 7-83), that describes the procedures agencies must follow to ensure adequate protection against unauthorized disclosure.

An additional due process question that is raised by verifying information from governmental or private sector (e.g., TRW or Dun & Bradstreet) databanks is: what recourse does the individual have if the information is false? Specifically, can the individual sue the databank owner or operator? The Privacy Act provides means by which individuals can take action against a Federal agency. The Fair Credit Reporting Act may provide a vehicle by which an individual could take action against a credit reporting agency. However, in other circumstances, statutes may not provide a legal means by which individuals can challenge false information and individuals would need to rely on common law defamation suits.

Finding 4

There has been no comprehensive study of how to conduct front-end verification in the most cost-effective manner and with the highest possible data quality.

The high costs of computer matching (e.g., verifying large numbers of hits, holding hearings, and prosecuting wrongdoers) are not incurred in front-end verification. However, front-end verification has its own costs. It may add to the caseworker's time in processing an application, although it may save somewhat in subsequent administrative time. Front-end verification will increase budgets devoted to automated data processing and telecommunications. There are also some high initial overhead costs in terms of developing the databases used for verification (e.g., State Income

---

[21] Davis, op. cit., 1979.

Verification Eligibility Systems) and getting them on-line, and ongoing costs of keeping them up to date.

The Department of Health and Human Services' survey of front-end eligibility verification techniques at the State level asked respondents about both developmental and operating costs. Most States were not able to provide the information as they were not keeping track of the administrative time devoted to verification.[22]

The major savings associated with front-end verification result from the avoidance of payments. The General Accounting Office reported that a New York State program that matched welfare applications with tax records to verify income avoided paying over $27.5 million, and that front-end verification in AFDC and food stamp programs in Arkansas saved $5 to $8 million.[23] In neither case was a detailed cost-benefit analysis available.

Another projected saving is a reduction in efforts to detect fraud, waste, and abuse for those already enrolled in government programs, as these individuals would have been initially screened by front-end verification. However, front-end verification would not eliminate the need to use other techniques (e.g., computer matching) because even when information is verified initially, frequent status changes (e.g., address and income) may necessitate later verification.

The President's Council on Integrity and Efficiency has projected that the eligibility verification required by the Deficit Reduction Act will save $1 billion over 5 years. The Congressional Budget Office did a gross estimate that confirmed this figure, but did not specify categories or figures for costs and savings.[24]

The costs of front-end verification are directly tied to data quality. The timeliness of data used is an especially critical issue; for example, wage data are often between 3 and 6 months out of date by the time they are available from State wage reporting agencies. Unearned income from the IRS is not reported until a month after the end of the tax year and would not be processed and available for verification purposes until many months later. Other income data can likewise be stale. Some front-end verification systems, such as those required in the Deficit Reduction Act, require workers to manually check information that appears false. However, the costs associated with front-end verification will increase with each subsequent verification.

Finding 5

At the present time, there are no policy guidelines for use of computer-assisted front-end verification.

There are no general Federal guidelines, statutory or administrative, guiding the use of front-end verification. The OMB computer matching guidelines specifically exclude from their purview record searches that are conducted at the application stage. The Deficit Reduction Act due process requirements for notice, verification, and hearings may provide a model for more general guidelines. In designing policy guidelines, the following factors warrant consideration:

1. *The responsibility for determining access to and record quality of the databases used for verification purposes.*

It is noteworthy that the FBI has taken the position that it has a responsibility only for the quality of the Triple I index entries, and not for the State criminal history records on which the index entries are largely based. Likewise, NHTSA officials have stated that the quality of driver's license records maintained by the States (and indexed in the NDR) is not the responsibility of NHTSA.

When records are maintained in a central Federal records repository, access and dissemination generally follow applicable Federal laws and regulations. However, under a decentralized index approach, record access and dissemination are much more complicated. There are wide differences in State laws and regulations on record access and dissemination, ranging all the way from so-called "open record" States such as Florida, where many personal records maintained in State files are open to public access at a modest fee, to very restrictive States like Massachusetts, where access and dissemination are tightly controlled.

---

[22] Interview with Liz Handley, Project Director, Department of Health and Human Services Front-End Eligibility Project, Apr. 9, 1985.

[23] U.S. General Accounting Office, *Eligibility Verification and Privacy in Federal Benefits Programs: A Delicate Balance*, HRD-85-22, Mar. 1, 1985.

[24] U.S. Department of Health and Human Services, Office of the Inspector General, *Semiannual Report to the Congress*, Apr. 1, 1985-Sept. 30, 1985.

This wide disparity in approach is especially true with respect to criminal history records, but also affects many other kinds of personal records maintained in State repositories. This contributes to inconsistent and incomplete exchange of record information. In some of the Federal social service and welfare programs, Congress has addressed this problem by requiring States to collect and exchange information as a condition of Federal funding, as discussed earlier. But in other areas such as criminal history records, while Congress previously has taken action to encourage enactment of State laws, there are wide differences among the many State laws that have been enacted.

2. *The frequency of use of front-end verification, i.e., routine or selective.*

If it is conducted routinely (e.g., for all benefit programs and Federal employment, loans, and contracts), the societal implications of subjecting to scrutiny all information submitted to the government by individuals would need to be considered. Any possible long-term societal effects, such as increased distrust between citizens and government, loss of individual responsibility, and a sophisticated governmental information infrastructure would need to be weighed against the significant budgetary savings that may be achieved by routine verification.

If front-end verification is used selectively (e.g., by law, OMB regulations, or court decisions) rather than routinely, then consideration must be given to the criteria for selecting Federal programs that may use it, the approval process for each use, and the societal groups that will be most affected. Another alternative for doing selective verification would be to select particular individuals rather than particular programs. The individuals selected for front-end verification could be chosen by a computer profile. However, profiling raises additional policy issues, as will be discussed in chapter 5.

3. *The rights of individuals.*

Based on due process principles, as well as traditional information privacy principles, individuals should be given some notice of verification and some means to challenge information if discrepancies should appear as a result of verification. There are a number of ways in which compliance with these principles could be achieved. Individuals could be informed in writing or verbally at the time they submit an application that the information supplied will be verified. Additionally, they could be given a range of details concerning the sources to be accessed in the process. Individuals wanting more details on the process or wishing to contest verification could be advised by the caseworker whom they should consult within the agency and when.

If front-end verification reveals problems with the information provided by the individual, then a process of further checking the validity of information and informing the individual of the problems could be started. The degree of individual involvement and the depth of validation may vary based on agency directives or the goodwill of caseworkers, and therefore may need to be specified in the regulations.

Once these principles are recognized in procedural protections, there may also be a need to ensure that agencies are providing the requisite notices and hearings. Some method of enforcement or automatic accounting could also be specified in the regulations. Such oversight could be conducted within the agency or by some outside body.

With respect to involving the individual in the verification of information, the Department of Education is conducting an experimental program, the Pell Grant Electronic Pilot.[25] Under this project, Pell Grant applicants can correct or verify information on their Student Aid Reports through computer facilities at institutions or financial aid services that participate in the project. Applicants can now make corrections on their Student Aid Reports and mail them back to the Department of Education.

4. *The types of information used.*

This question involves whether the use of some types of information (e.g., medical history or criminal history) should be prohibited because of their sensitivity. The use of such information could be prohibited, or its use could be restricted to particular verifications, for example, use of criminal history information in screening day-care workers.

Additionally, front-end verification raises a separate and potentially more serious issue because the information is being used to make an immediate, or near immediate, decision. In order for front-end verification to be most effective, information should be up to date, accurate, and complete. However, the information in some categories, for example, unearned income and checking accounts, may change so often that the data contained in computerized databanks will rarely be up to date. Additionally, the record quality of many existing databanks that could be used in front-end verification (e.g., computerized criminal history records) is questionable.

5. *The possible requirement of a cost-benefit analysis.*

Because a major purpose of front-end verification is to cut programmatic costs, documentation of how front-end verification will achieve this may be necessary. If a cost-benefit analysis were to be required, the categories of costs and benefits to be included could be specified in regulations. The detail to which costs and benefits should be analyzed could also be specified. The degree of detail may vary depending on the category; for example, administrative costs may be more difficult to compute than telecommunication costs.

Cost-benefit analyses could be used within an agency or program for internal improvements in ongoing front-end verifications. They could also be distributed among agencies or programs for development of new front-end verifications. Additionally, they could be used within an agency or by an outside body as part of a process of approval of new front-end verifications or review of ongoing ones.

---

[25] U.S. Department of Education, Office of Postsecondary Education, "Invitation To Participate and Closing Date for Participation in Pell Grant Electronic Pilot," *Federal Register*, vol. 50, No. 141, Tues., July 23, 1985.

Chapter 5
Computer Profiling

Contents

Page
Summary 87
Background 87
Findings 89
  Finding 1 89
  Finding 2 91
  Finding 3 93
  Finding 4 94

Chapter 5

Computer Profiling

SUMMARY

While computer profiling is not currently a subject of major policy debate, the potential policy issues raised by the future growth of computer profiling are important. In computer profiling, a record system (or record systems) is searched for a specified combination of data elements, i.e., the profile. Profiling involves the use of inductive logic to determine indicators of characteristics and/or behavior patterns that are related to the occurrence of certain behavior.

A profile is developed by a government agency to select characteristics of types of individuals, and to determine the probabilities of such individuals engaging in activities or behavior of interest to that agency. For example, the Drug Enforcement Agency (DEA) has developed profiles of the types of persons more likely to be engaging in illegal drug activity; the Internal Revenue Service (IRS) has developed profiles of categories of taxpayers more likely to be under-reporting taxable income; and the Federal Bureau of Investigation (FBI) has developed profiles of violent offenders. Profiles can be valuable tools for investigative, administrative, and intelligence purposes because they reduce the population that is of interest to an agency, and thus may increase the agency's efficiency and effectiveness.

OTA found that:

- Federal agencies are currently using computer profiling and it is likely that its use will expand in the near future.
- Important privacy and constitutional implications are raised by computer profiling because people may be treated differently before they have done anything to warrant such treatment.
- The validity of computer profiles in accurately selecting the desired subset of individuals is subject to debate, and thus also raises questions about the relevancy of data used and the appropriateness of using computer profiles for certain decisions.
- At the present time, there are no policy guidelines for agency use of computer profiling.

BACKGROUND

Before computers were used to process and store information, systematic data on large numbers of individuals were not retained (or if retained were not readily accessible). Moreover, there was no easy means to analyze the data that did exist in order to construct profiles. Information technology in general—and computers in particular—have removed these constraints. Detailed, historical information on individuals can be compiled from various computerized databases. Computers can be used to analyze complex and disparate information and, based on that analysis, to design a profile. Additionally, computers can be used to search a record system on the basis of a profile. These technological changes make profiles both more powerful and more available. Most importantly, technology is now making possible many new profiling applications for which judgments of social acceptability have yet to be made.

Profiling involves the use of inductive logic to determine indicators of characteristics and/or behavior patterns that are related to the occurrence of certain behavior. A judgment is made about a particular individual based on the past behavior of other individuals who appear statistically similar, that is, who have similar demographic, socioeconomic, physical, or other characteristics. Generally, in the Federal Government, the behavior of interest is actual or potential violation of a law or administrative regulation.

In the past, and as is often still the case, people who appeared suspicious or acted strangely were often watched more carefully and their stories were verified from outside sources. Searches through Federal record systems were often conducted on the basis of a list of characteristics that experience had shown were problematic. Such profiles were often crude and could easily lead to the stereotyping of individuals. Today, profiling is much more sophisticated as a result of advances in behavioral psychology and statistics. As most behavior is complex, sophisticated modeling may be done to determine the interrelations among certain indicators. There are two general models of profiling. One is singular profiling, which models distinct characteristics or activities, e.g., sex, age, income, or number of dependents. When these characteristics appear together or in a certain pattern, that individual is flagged by the profile. The second model of profiling is aggregative profiling, which is based on the frequency with which selected factors appear across cases. This model is designed to find systematic and repetitive violators.[1]

Profiles have been used for decisionmaking in a variety of areas, ranging from insurance and advertising to motor vehicle or real estate licensing to entrance to the medical and legal professions. Profiles used range from those that are benign and socially acceptable (e.g., granting driver's licenses to 16 year olds, who in most States are judged to be physically and mentally mature enough to drive a car) to those that are discriminatory and socially unacceptable (e.g., denying rental housing to minorities or students or denying professional employment opportunities to women).

Profiles have been used by the government to help agencies uncover possible misrepresentation of eligibility to receive Federal funds or benefits, possible noncompliance with or violation of agency regulations, and possible violation of civil or criminal statutes. In the government, profiles can be created, to some extent, for the convenience of implementing public policies, as they replace subjective judgments with objective decisionmaking criteria. Profiles can be useful during any stage of an agency's interaction with individuals. For example, in eligibility benefit programs, profiling may be used at the application stage to determine if an applicant is likely to misrepresent his or her income, or at the redetermination stage to ascertain if it is likely that an individual's status has changed. In law enforcement, profiling may be used in discovering likely suspects (e.g., airplane hijackers) or in determining an appropriate sentence for someone convicted of a crime. Profiles can be valuable tools for investigative, administrative, and intelligence purposes because they reduce the population that is of interest to an agency, and thus may increase the agency's efficiency and effectiveness.

Because computer profiling may result in selected individuals being treated differently from those not selected, it has raised a number of policy questions involving civil, constitutional, and equal rights considerations. The primary conflict is between the rights of the individuals selected (e.g., equal protection and due process) and the purpose of the government in using computer profiles and their effectiveness in achieving that purpose. No matter how sophisticated the profile, the question of treating people differently before they have acted remains.

Computerized profiling also introduces some very important new policy issues. If the use of computer profiling in the Federal Government were to be expanded, the long-term societal effects on behavior patterns, and the possible effects on individuality and creativity, would warrant attention. Additionally, the validity of computer profiles in accurately selecting the desired subset of individuals is subject to debate, and thus also raises questions about the relevancy of data used and the appropriateness of using computer profiles for certain decisions.

---

[1] Gary T. Marx and Nancy Reichman, "Routinizing the Discovery of Secrets," *American Behavioral Scientist*, vol. 27, No. 4, March/April 1984, pp. 429-431.

FINDINGS

Finding 1

Federal agencies are currently using computer profiling and it is likely that its use will expand in the near future.

Federal agencies have developed profiles for a number of purposes, mainly for identifying individuals most likely to be involved in an illegal activity or most likely to misrepresent their financial or personal situation in applying for a Federal benefit. The OTA survey revealed that 16 Federal agencies presently use computer profiling. For example, the IRS uses computer-generated generic profiles to identify potential compliance deficiencies; the Department of Education uses profiles, based on criteria including taxes paid, marital status, and size of household, to select Pell Grant applicants for validation; the Bureau of Indian Affairs profiles the public social service support and facilities usages and needs of individual corporate groups of Indians for budgetary planning and allocation of resources; and the Federal Reserve Board uses surveys of retailers and consumers to obtain statistical data concerning financial status and behavior of households and businesses, access to and use of consumer credit, asset holdings, financial practices, effect of charge card transactions, and the like.

According to the OTA survey, some agencies are planning to add this capability to existing systems. For example, the redesign of the Treasury Enforcement Communications System, known as TECS II, will incorporate profiling. The U.S. Army Criminal Investigation Command is considering developing a system of profiling potential victims and criminal offenders for use in the conduct of crime prevention surveys and in the development of investigative leads. Some agencies have conducted pilot programs of profiling that are no longer in use, for example, the Office of the Inspector General in the Department of Energy developed, with DOE Defense Programs, a profile of the "Insider Criminal."

The use of profiles for law enforcement purposes has been widely documented. Computers were not necessarily used in preparing these, but they are illustrative of the type of computer profiles already under development. The Drug Enforcement Agency (DEA) has developed a profile of airplane passengers likely to be smuggling drugs, and a profile to detect those transporting marijuana on trains.[2] The Coast Guard has a profile of vessels likely to be smuggling drugs into the country.[3] The Customs Bureau also has a "smuggler's profile."[4] The Federal Aviation Administration used a hijacker profile as part of its screening program at domestic airports until it began routine searches of all carry-on items and magnetometer screening of all passengers.[5]

The FBI has developed numerous profiles, including those of various violent criminals and serial murderers. This work is being expanded under the auspices of the FBI's National Center for the Analysis of Violent Crimes. Also, based in large part on interviews with felons convicted of serial murders, the FBI has developed profiles of serial murderers, especially serial sex murderers.[6] The FBI is currently developing software for preparing computerized profiles of violent offenders, based on the concept already implemented for arson offenders in the computer-assisted Arson Information Management System (AIMS).[7] In 1983, the Office of Juvenile Justice and Delinquency Prevention of the Department of Justice funded the University of Pennsylvania School of Nursing to identify the variables that fit profiles of rapists, child molesters, and sexually exploited children.[8]

---

[2] See, for example, *United States v. Johnston*, 497 F.2d 397 (9th Cir. 1974) and *United States v. Chadwick*, 393 F. Supp. 763 (D. Mass. 1975).

[3] Note, "High On the Seas: Drug Smuggling, the Fourth Amendment, and Warrantless Searches at Sea," *Harvard Law Review*, vol. 93, 1980, p. 725.

[4] See, for example, *United States v. Klein*, 592 F.2d 909 (5th Cir. 1979), and *United States v. Asbury*, 586 F.2d 973 (2d Cir. 1973).

[5] Note, "The Airport Search and the Fourth Amendment: Reconciling the Theories and Practices," *U.C.L.A.—Alaska Law Review*, vol. 7, 1978, p. 307.

In the 1970s, the Law Enforcement Assistance Administration funded "pre-delinquency" programs to create computer models to identify those young people who were likely to become delinquent. The computer models or profiles included factors that were common among known delinquent youths, such as area of residence, family situation, school performance, ethnic group, and medical history. Young people who most closely matched the profile were to be given special treatment. In 1983, the Office of Juvenile Justice and Delinquency Prevention funded the Rand Corp. to develop strategies based on the "pre-delinquency" presumption.

Computer profiles can also be used as a way of avoiding errors in Federal Government eligibility and benefit programs and as a way of allocating scarce investigative resources. Based on a computer profile, caseworkers can determine during the application process which applicants may need more careful checking. Characteristics often associated with errors could include basic factors such as age, race, or education level; some combination of factors; or more indirect factors, such as length of family separation, residency, or living with a specified relative. In 1979, the Supplemental Security Income's Office of Family Assistance reported that the following characteristics were used in error-prone profiles: earned income, home ownership, age 26 to 40, recent separation, bank account, and overdue redeterminations of benefits.[9]

In eligibility benefit programs, computer profiles or screens can also be used to search databases of recipients prior to conducting a computer match. The records that were selected by the profile would be the only ones subject to computer matching. A smaller number of records would then be matched. If the computer profile was effective in selecting those records most likely to contain errors, then the percentage of verifiable hits would increase. In this way, computer profiles or screens may make computer matching more effective and efficient. Additionally, cuts in the Federal budget may increase the pressure to use computer profiling not only to detect and prevent fraud and errors, but also to allocate the time of caseworkers or investigators.

There has been no survey of the use of computer profiles in social service programs at the Federal level. The President's Council on Integrity and Efficiency (PCIE) has released three inventories of Federal computer applications to prevent/detect fraud, waste, and mismanagement. The applications include matches, profiles, edits, scans, screens, analyses, and extracts. If one adopts the PCIE categorization, there were no profiles used prior to 1982, 13 profiles used in the period 1982-83, and five profiles used in the period 1984-85.[10] However, agencies have sometimes placed computer applications that appear to be profiles in a different category, e.g., Project Sonoma—Welfare Fraud Profile is listed as a match. Some computer screens appear to be based on a computer profile (e.g., a Department of Education screen designed to identify, by selected criteria, guaranteed student loans maintained by State Guaranty Agencies that are in excess of the regulatory maximum of 10 years), while others do not (e.g., prescription payments made by Blue Cross and Blue Shield, screened to ascertain whether that company was computing and claiming Medicaid prescription drugs in accordance with Federal procedures).

---

[6] Robert K. Ressler, Ann W. Burgess, Ralph B. D'Agonstino, and John E. Douglas, "Serial Murder: A New Phenomenon of Homicide," September 1984.

[7] AIMS deals both with past activities, in developing profiles on arson incidents, and possible future activities, in profiling arson-prone properties and suspects. See U.S. Fire Administration, *Arson Information Management System: Users Manual and Documentation*, Apr. 2, 1984.

[8] "Pre-Delinquent Funding: Déjà Vu," *Privacy Journal*, April 1984, p. 3.

[9] "Use of Error Prone Profiles," *Eligibility Simplification Project*, October 1980.

[10] U.S. Department of Labor, Office of Inspector General, "Inventory of Federal Computer Applications To Prevent/Detect Fraud, Waste and Mismanagement." Original distributed July 1982; supplements distributed July 1984 and January 1986.

Information on State use of computer profiles is also sketchy. The Carter Administration's Eligibility Simplification Project reported on the use of error-prone profiles, primarily at the State level. According to its study, West Virginia had used computer profiling, or a selective case action system, for Aid to Families With Dependent Children (AFDC), food stamp, and Medicaid cases, based on a quality-control sample generated monthly by the computer. The profile was based on a statistical method of evaluating previous error situations and was modified periodically. Reportedly, from 1973 to 1976, the case error rate and payment error rate declined by 20 percent.[11] The Eligibility Simplification Project found similar results with the use of error-prone profiling in South Carolina and New Hampshire. The Eligibility Simplification Project found that other States appeared to be experimenting with the use of such profiles in determining social service eligibility. A survey of seven States conducted for OTA in 1984 revealed that computer profiling was not used by those States.[12]

Finding 2

Important privacy and constitutional implications are raised by computer profiling because people may be treated differently before they have done anything to warrant such treatment.

Computer profiles involve categorizing people based on selected criteria, and then selecting a subset of these people for special treatment. The equal protection guarantees of the fifth and 14th amendments were designed to ensure that individuals were treated in a manner similar to other individuals, and that the government not treat individuals differently simply because they were members of a group. Although the government can classify people for special treatment, it cannot do so based on impermissible criteria (e.g., race, religion, or national origin), nor can it use a classification to arbitrarily burden a group of individuals. In computer profiling, the criteria used might be those that are already viewed as discriminatory under existing law—e.g., race, religion, national origin, and sex. For example, in DEA's drug courier profile, being Hispanic has appeared as one of the criteria. With sophisticated profiling, it may also be possible to use a number of related indicators rather than a category whose use would be illegal.

The equal protection clauses may also require that the criteria on which the profile is based be related to the behavior in question; otherwise, the selected group may be arbitrarily burdened. Additionally, the government's program would need to be rationally related to achieving a legitimate purpose such as detecting fraud, waste, and abuse or apprehending drug smugglers.

The use of computer profiling may also conflict with the due process clauses of the fifth and 14th amendments that protect an individual against arbitrary treatment and provide an individual with certain procedural guarantees. Some argue that computer profiles eliminate the discretion and arbitrariness of investigative authorities, caseworkers, and parole officers. Others respond that profiles merely replace a crude form of profiling (hunches, for example) with a more sophisticated one. In either case, the due process clauses require rules and procedures to limit discretion and protect individuals from arbitrary treatment. In some instances, use of computer profiling may not provide for adequate rules and procedures.

With respect to the use of profiles in eligibility programs, Senator William Cohen reported that:

---

[11] Ibid.

[12] Robert Ellis Smith, "Report on Data Protection and Privacy in Seven Selected States," OTA contractor report, February 1985. The seven States are California, Florida, Indiana, Minnesota, New York, Texas, and Virginia.

> We have profiles that have been developed by computer, and disability payments that have been discontinued with no human contact coming about until such time as those cases are appealed to an administrative law judge. Two-thirds of the cases appealed are being reversed.[13]

The extreme result of a computer profile would be that benefits are terminated, which would not occur without a hearing. The more common result would be that a selected individual is subject to a more thorough investigation than others because he or she fits a profile. To some extent, this individual is regarded with suspicion based on the profile. Individuals may not know that they are being treated differently, and even if they do, may not know why.

With respect to the use of computer profiles in law enforcement, the primary issue is whether fitting a profile constitutes probable cause or reasonable suspicion and is reason to search or detain an individual. In determining whether an investigative stop is lawful, the courts balance the need for the search against the intrusion to the person. To justify the intrusion, law enforcement agents must be able to identify specific and articulable facts that show the intrusion is reasonably warranted.[14]

There have been a number of court cases involving the use of the drug courier profile, and, hence, this will serve as an example of the legal issues that arise with use of profiles for law enforcement purposes. Although this profile is not currently generated by a computer nor are computers necessarily used to search relevant databases, the legal issues would be similar whether or not a computer was involved. Agents typically use the drug courier profile as a tool in conducting surveillance on a group of people, generally those boarding or departing a plane. If agents see a person whose behavior fits a number of criteria in the profile, then they follow the person. If agents believe it is justified, they stop the individual, identify themselves as law enforcement agents, and request to see identification. Based on the information revealed and the behavior of the person, the agents may then "request" that the suspect accompany them to an office in the airport. There the person is told that he or she is suspected of carrying drugs, advised of his or her rights, and asked for permission to search his or her luggage and person.[15]

In cases in which the sole or primary justification for an investigative stop has been the drug courier profile, the lower courts have not been consistent in their rulings. For example, in *United States v. McCaleb*, 552 F.2d 717 (6th Cir. 1977) and *State v. Washington*, 364 So. 2d 958 (La. 1979), the courts reversed the appellants' convictions based on investigative stops triggered by meeting a drug courier profile because their activities were too consistent with innocent behavior. In *United States v. Vasquez*, 612 F.2d 1338, an investigative stop based in part on a profile was judged valid.

In 1979, the Supreme Court ruled on two instances involving the use of the drug courier profile. In the first case, *United States v. Mendenhall*, 446 U.S. 544, the Court ruled that the investigative stop of Mendenhall, which was based on her fitting characteristics of the drug courier profile, was constitutional. However, the majority did not agree on why it was constitutional, giving little guidance to the lower courts on the acceptability of the profile in establishing justification for an investigative stop. One month later, the Court handed down a second decision dealing with the drug courier profile, *Reid v. Georgia*, 448 U.S. 438. In this case, the Court held that the investigative stop of Reid, based on his matching characteristics of the drug courier profile, was not constitutional. The Court described the drug courier profile as "a somewhat informal compilation of characteristics believed to be typical of persons unlawfully carrying narcotics."[16]

---

[13] Senate Committee on Governmental Affairs, Subcommittee on Oversight of Government Management, *Oversight of Computer Matching To Detect Fraud and Mismanagement in Government Programs*, hearings, Dec. 15-16, 1982 (Washington, DC: U.S. Government Printing Office, 1982), p. 17.

[14] *Terry v. Ohio*, 392 U.S. 1 (1968).

[15] For a description of the profile, its use, and court cases, see William V. Conley, "*Mendenhall* and *Reid*: The Drug Courier Profile and Investigative Stops," *University of Pittsburgh Law Review*, vol. 42, summer 1981, pp. 835-867; Hon. Mark A. Costantino, Vito A. Cannavo, and Ann Goldstein, "Drug Courier Profiles and Airport Stops: Is the Sky the Limit?" *Western New England Law Review*, vol. 3, 1980, p. 175; Philip S. Greene and Brian W. Wice, "The D.E.A. Drug Courier Profile: History and Analysis," *South Texas Law Journal*, vol. 22, spring 1982, p. 261; Kathleen Mahoney, "Drug Trafficking at Airports—The Judicial Response," *University of Miami Law Review*, vol. 36, 1981, p. 91; and Francis Karl Toto, "Drug Courier Profile Stops and the Fourth Amendment: Is the Supreme Court's Case of Confusion in Its Terminal Stage?" *Suffolk University Law Review*, vol. 25, 1981, p. 217.

Based on these two cases, the legal status of the present drug courier profile is in question. Moreover, the *Reid* opinion may imply that the constitutionality of the profile could turn on its sophistication. If this is true, then the use of computer-generated profiles in law enforcement may be considered a more valid investigative tool than the more informal profiles.

Federal court decisions since *Mendenhall* and *Reid* have not clarified the status of the use of a drug courier profile in an investigative stop.[17] In 1981, in *United States v. Cortez*, 101 S.Ct. 690, the Supreme Court approved use of a profile by border patrol agents to detect the smuggling of illegal aliens from Mexico to the United States.

Finding 3

The validity of computer profiles in accurately selecting the desired subset of individuals is subject to debate, and thus also raises questions about the relevancy of data used and the appropriateness of using computer profiles for certain decisions.

Profiles vary in their complexity and in the formality of statistical techniques on which they are based. Because computers are such powerful tools in analyzing and manipulating vast quantities of data, it is likely that profiles will become even more complex and formal. Regardless of their complexity and formality, profiles by definition are prone to some degree of error, as they are merely probability statements.

In formal profiles, when a general population is characterized and a profile developed the profile is only a statistical average of that general population. The similarities among the population will be accentuated, while the differences will be ignored. If the profile was based on a sufficiently large population, it will have *some* value in selecting those of interest, but there will also be some margin of error in the profile. The types of errors will be false positives (identifying those who fit the profile, but do not fit the category sought) and false negatives (passing by those who do not fit the profile, but do fit the category sought). In developing the profile, the statistician will incorporate the degree of error that the user is willing to tolerate.

The more informal, crude profiles are greatly influenced by the experience and concerns of those who develop them. For example, in the case of the drug courier profile, the criteria that make up the profile have varied over time and with the city in which DEA agents are working. Some subset of the following are generally considered as the profile: the use of small bills for ticket purchase, travel to and from major drug import centers, travel for short periods of time, absence of luggage or empty luggage, travel under an alias, unusual itinerary, unusual nervousness, use of public transportation, making a phone call after deplaning, leaving a fictitious callback telephone number with the airline, attempting to conceal that someone is waiting for them or that they are traveling with someone, purchase of a one-way ticket, Hispanic origin, youth, luggage without identification tags, ticket purchased at the last minute or late arrival, and deplaning last. There is no record establishing how and why these characteristics have come to be included in the profile. There may also be some criteria that DEA keeps confidential.

The OTA survey asked agencies to provide both information on the development and testing of profile programs and any evaluation reports. Of the 16 agencies that reported profiling activities, none had this information available. There are no known studies of the degree of error in profiles used in eligibility verification programs.

---

[16] *Reid v. Georgia*, 448 U.S. 438, 440.

[17] See: *United States v. Fry*, 622 F.2d 1218 (5th Cir. 1980), *United States v. Robinson*, 625 F.2d 1211 (5th Cir. 1980), and *United States v. West*, 495 F.Supp. 871 (D. Mass. 1980).

A principal policy issue involves determining the accuracy of a computer profile and its effectiveness in achieving the desired outcome. The cost-effectiveness of computer profiles has never been systematically studied. There are a number of costs that may need to be considered: 1) developmental costs, including research, testing, validation, and evaluation; 2) computer costs, including hardware and software; and 3) administrative costs, including follow-up on individuals who fit the profile. The costs to individuals who may needlessly be subject to investigation may also need to be considered. Additionally, as with computer matching, there may be hidden or secondary costs that need to be examined.

There are also a number of benefits that need to be considered, primarily increasing the effectiveness and efficiency of an investigation because the relevant population has been narrowed, and preventing and deterring illegal behavior.

Some information is available on the effectiveness of profiling for law enforcement purposes. None contains specific cost-benefit categories or figures. A 1981 FBI evaluation of psychological profiling found that, of 192 cases examined, in 77 percent the profile helped focus the investigation, in 20 percent it helped locate possible suspects, and in 17 percent the profile actually identified the suspect. (Totals exceed 100 percent since more than one type of assistance may apply to a single case.) The vast majority of cases were murder or rape investigations.[18]

There are some sketchy statistics on the effectiveness of the drug courier profile in selecting persons carrying drugs. In *United States v. Van Lewis*, 409 F.Supp. 535 (E.D. Mich. 1976), testimony from DEA revealed that agents at the Detroit airport had searched 141 persons in 96 encounters, found narcotics in 77 of these encounters, and arrested 122 persons. Forty-three of the searches in which narcotics were found were nonconsensual. In 15 of the 25 consent searches, no illegal narcotics were found.[19] In testimony in *United States v. Price*, 599 F.2d 494 (2d Cir. 1979), a DEA agent stated that about 60 percent of those he stopped, based on the drug courier profile, were carrying narcotics. However, it appears that no national statistics are available on the effectiveness of the drug courier profile.

Finding 4

At the present time, there are no policy guidelines for agency use of computer profiling.

The use of computer profiling raises a number of important policy questions. In determining the appropriate use of computer profiling, a number of factors warrant consideration, including:

1. The *nature of the decision* for which the profile is used. In other words, under what circumstances is it appropriate to use computer profiling? In answering this question, two distinctions may prove helpful. The first is the government's purpose in using profiling—e.g., detection of fraud, waste, and abuse; detection of violent criminals; and detection of discrimination. It may be appropriate to use computer profiling for all of these purposes and for any other purposes. Alternatively, the dangers of categorizing people and the speculative nature of profiles may outweigh their general use, but not their use for specific purposes.

   The second distinction is whether only one individual, or one group or class of individuals, is subject to the computer profile. A profile may provide the key by which a database of many individuals is searched. One individual may also be selectively compared to a profile. Because an individual may be affected differently under the two circumstances, different standards could be considered for its use.

---

[18] Federal Bureau of Investigation, "Evaluation of the Psychological Profiling Program," December 1981.

[19] Conley, "*Mendenhall* and *Reid*," op. cit., p. 839.

2. The *nature and source of the data* used. To be consistent with equal protection law, one could argue that computer profiles should not include criteria traditionally considered discriminatory, e.g., race, religion, national origin, or sex. It may also be necessary to eliminate or restrict the use of attributes that may substitute for the overtly discriminatory criteria. Additionally, it may be necessary to restrict the use of results of sophisticated invasive or intrusive psychological or physiological tests, e.g., genetic testing, in profiles.

   In setting standards for the use of data, it may also be helpful to consider the source of the data in determining its relevance for a profile. For example, it may not be appropriate for IRS profiles to include information not provided by the taxpayer or not directly relevant to financial matters.
3. The *rights of individuals*, with respect to both decisions based on profiles and being the subject of profiling, regardless of use. Should individuals be informed that their records are being searched on the basis of a profile or that they are being compared to a profile? If they do not want to be subject to profiling, what are their remedies? If an individual is accorded different treatment because of the way he or she compares to a profile, what rights does he or she have and how can they be implemented?
4. The *accuracy* of the profile. Given that profiles themselves are prone to errors, some testing may be necessary prior to the use of a profile. Independent validation and testing of any software program used for profiling may be necessary to determine bias and accuracy. If profiles are to be used, guidelines may need to be developed for validation and testing. It may be necessary that this testing be done by a group (or groups) other than the one that developed the profile. Although it may be difficult to get an exact accounting of costs and benefits, some outlining of the significant costs and benefits that are expected could also be done.

   With respect to the drug courier profile, William Conley has suggested that testing should be done in two steps. First, establishing the percentage of those previously arrested who displayed a particular characteristic. Second, determining what percentage of all airplane passengers exhibit the same characteristic.[20]

---

[20] Ibid., p. 863.

Chapter 6

Policy Implications

Contents

Page
Summary 99
Introduction 100
Policy Problems 104
Policy Actions 107
  Action 1: Maintaining the Status Quo 107
  Action 2: Problem-Specific Actions 108
  Action 3: Institutional Changes 113
  Action 4: Consideration of a National Information Policy 122

Table

Table No. *Page*
15. Selected Institutional Changes for Information Policy Proposed in the 99th Congress 123

Chapter 6

Policy Implications

SUMMARY

All governments collect and use personal information in order to govern. Democratic governments moderate this need with the requirements to be open to the people and accountable to the legislature, as well as to protect the privacy of individuals. In the United States, these needs are recognized in the Constitution and various public laws.

In 1974, Congress passed the Privacy Act to address the tension between the individual's interest in privacy and the government's need to know. Since the act was passed, there have been dramatic changes in the scale and scope of technological innovations applied to records and record systems, primarily as a means to detect fraud, waste, and abuse, and to aid in law enforcement investigations. New technological applications—most notably the widespread use of microcomputers, computerized record searches, and computer networking—have multiplied within Federal agencies, and have expanded the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information. Individual rights and remedies, as well as administrative responsibilities, are not clear under current policies. At the same time, there is stronger public concern for privacy and more support for legislative protections than there was in the past.

OTA's analysis of Federal use of electronic record systems revealed a number of common policy problems. First, new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves. Second, there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal compliance with the Privacy Act and related Office of Management and Budget (OMB) guidelines. Third, neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved. Fourth, within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered.

Overall, OTA has concluded that Federal agency use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many applications of electronic records being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered either by the act or subsequent OMB guidelines. Moreover, the use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a *de facto* national database containing personal information on most Americans. And use of the social security number as a *de facto* electronic national identifier facilitates the development of this database. Absent a forum in which the conflicts generated by new applications of information technology can be debated and resolved, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

Additionally, OTA's analysis of electronic record systems and their effect on individual privacy has confirmed once again the complexity of Federal information policy. Its broad social, economic, and political implications need systematic policy study.

OTA identified a range of policy actions for congressional consideration:

1. Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion. This

would lead to continued uncertainty regarding individual rights and remedies, as well as agency responsibilities. Additionally, lack of congressional action will, in effect, represent an endorsement of the creation of a *de facto* national database and the use of the social security number as a *de facto* national identifier.

2. Congress could consider a number of problem-specific actions. For example:
   - establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of personal information, and the rights of individuals;
   - implement more controls and protections for sensitive categories of personal information, such as medical and insurance;
   - establish controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government and provide for appropriate enforcement mechanisms;
   - review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness;
   - review issues concerning use of the social security number as a *de facto* national identifier and, if necessary, restrict its use or legislate a new universal identification number; or
   - review policy with regard to access to the Internal Revenue Service's (IRS) information by Federal and State agencies, and policy with regard to the IRS's access to databases maintained by Federal and State agencies, as well as the private sector. If necessary, legislate a policy that more clearly delineates the circumstances under which such access is permitted.
3. Congress could initiate a number of institutional adjustments, e.g., strengthen the oversight role of OMB, increase the Privacy Act staff in agencies, or improve congressional organization and procedures for consideration of information privacy issues. These institutional adjustments could be made individually or in concert. Additionally or separately, Congress could initiate a major institutional change, such as establishing a Data Protection or Privacy Board or Commission.
4. Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which information privacy is a part.

INTRODUCTION

All governments collect and use personal information in order to govern. Democratic governments moderate this need with the requirements to be open to the people and accountable to the legislature, as well as to protect the privacy of individuals. Advances in information technology have greatly facilitated the collection and uses of personal information by the Federal Government, but also have made it more difficult to oversee agency information practices and to protect the rights of individuals.

In the 1960s, Congress and the executive branch began the first modern reexamination of the effects of government information collection on individual privacy and agency accountability. This occurred in response to two factors: first, the explosion in information activities necessitated by the Great Society programs; and second, the introduction in Federal agencies of large mainframe computers for information storage and retrieval. This reexamination went on for a number of years, and included, most prominently, the 1966 and 1967 hearings on the proposal to establish a National Data Center,[1] the 1971 Senate Committee on the Judiciary hearings on Federal databanks,[2] the 1973 Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems,[3] and the 1972 project on databanks sponsored by the Russell Sage Foundation and the National Academy of Sciences.[4]

The reexamination of government information collection, computers, and privacy culminated in the 1974 joint hearings of the Senate Committee on Government Operations, Ad Hoc Subcommittee on Privacy and Information Systems and the Senate Committee on the Judiciary, Subcommittee on Constitutional Rights;[5] and hearings of the House Committee on Government Operations.[6] These hearings coincided with Watergate and its revelation of how those in power could use and abuse personal information, especially that held by the IRS and the Federal Bureau of Investigation, for their own personal advantage. The result of these hearings was the enactment of the Privacy Act of 1974, which established rights and remedies for individuals who are the subjects of agency recordkeeping and specified requirements that Federal agencies were to meet in handling personal information. In addition, OMB was assigned responsibility for overseeing agency implementation of the act.

Technology.—At the time the Privacy Act was debated and enacted, there were technological limitations on how agencies could use individual records. The vast majority of Federal record systems were manual. Computers were used only to store and retrieve, not manipulate or exchange, information. It was theoretically possible to match personal information from different files, to manually verify information provided on government application forms, and to prepare a profile of a subset of individuals of interest to an agency. However, the number of records involved made such applications impractical.

In the 12 years since enactment of the Privacy Act, at least two generations of information technology have become available to Federal agencies. Advances in computer and data communication technology enable agencies to collect, use, store, exchange, and manipulate individual records, as well as entire record systems, in electronic form. Specifically:

- Microcomputers were not used at all by Federal agencies in the 1970s. Agencies responding to the OTA survey reported a few thousand microcomputers in 1980, with a dramatic increase to over 100,000 in 1985.
- Computer matching was not used by Federal agencies until 1976, and from 1980 to 1984 there was almost a threefold increase in the number of computer matches. Computer matching has become routine in a number of programs, especially eligibility benefit programs.
- Use of computer-assisted front-end verification, especially with on-line computer searches, has intensified in the 1980s, particularly following the requirements of the 1984 Deficit Reduction Act.
- The widespread use of computerized data-

---

[1] U.S. Congress, House Committee on Government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and Invasion of Privacy*, hearings, 89th Cong., 2d sess., July 26, 27, and 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966); U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasions of Privacy (Government Agencies)*, hearings, 89th Cong., 2d sess., part 5, Mar. 23-30 and June 7-9, 14, and 16, 1966 (Washington, DC: U.S. Government Printing Office, 1967); and *Computer Privacy Hearings*, 90th Cong., 1st sess., Mar. 14-15, 1967 (Washington, DC: U.S. Government Printing Office, 1967).

[2] U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks, Computers and the Bill of Rights*, hearings, 92d Cong., 1st sess., Feb. 24-25 and Mar. 2, 3, 4, 9, 10, 11, 15, and 17, 1971, part 1 (Washington, DC: U.S. Government Printing Office, 1971).

[3] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[4] Alan F. Westin and Michael A. Baker, *Databanks in a Free Society* (New York: Quadrangle/New York Times Book Co., 1972).

[5] U.S. Congress, Senate Committee on Government Operations, Ad Hoc Subcommittee on Privacy and Information Systems, and Committee on the Judiciary, Subcommittee on Constitutional Rights, *Privacy—The Collection, Use and Computerization of Personal Data*, joint hearings, 93d Cong., 2d sess., June 18-20, 1974 (Washington, DC: U.S. Government Printing Office, 1974).

[6] U.S. Congress, House Committee on Government Operations, *Privacy Act of 1974* (Report 93-1416), 93d Cong., 2d sess. (Washington, DC: U.S. Government Printing Office, 1974).

bases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a *de facto* national database containing personal information on most Americans. And use of the social security number as a *de facto* electronic national identifier facilitates the development of this database.

- In the 1970s, manual profiling was used by a few agencies, especially for law enforcement purposes. In the 1980s, computers can be used to generate profiles, and software programs can search databases on the basis of these profiles. The use of computer profiling is expanding beyond law enforcement per se to include various management programs, such as those designed to detect fraud, waste, and abuse.

These technological advances have opened up many new possibilities for improving the efficiency of government recordkeeping; the detection and prevention of fraud, waste, and abuse; and law enforcement investigations. At the same time, the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. Because of this expanded access to and use of personal information in decisions about individuals, the completeness, accuracy, and relevance of information becomes even more important. Additionally, it is nearly impossible for individuals to learn about, let alone seek redress for, misuse of their records. Even within agencies, it is often not known what applications of personal information are being used. Nor do OMB or relevant congressional committees know whether personal information is being used in conformity with the Privacy Act.

Information Technology and Fair Information Principles.—The core of the Privacy Act of 1974 is the code of fair information principles. Twelve years later, it is important to review these principles in light of current information technology applications and administrative practices. Although there are a number of iterations of the code of fair information principles, the model for the Privacy Act was the one developed by the Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems, and hence will serve as the basis for the analysis here.

The first principle is that **there must be no personal data recordkeeping system whose very existence is secret**. Ensuring that all record systems containing personally-identifiable information are cataloged for the public record depends on each agency carefully monitoring its record systems. In an age of electronic record systems, it is difficult for an agency to keep an accurate catalog of all record systems, both because of the number of systems and because of the continual electronic changes and manipulations. Additionally, the multiplication of personal data systems makes it difficult for an individual to be aware of all the systems whose existence is public.

There are two types of record systems whose status under the Privacy Act is unclear. The first is a personal information system maintained on a microcomputer. Privacy Act officers are unsure of their responsibilities in this area and are looking for either legislative or OMB clarification.[7] The question is whether records maintained on microcomputers are analogous to "desk notes," which are not covered by the Privacy Act, or whether they are of a different character because they can be retrieved by others and easily disseminated.

The second type of record system whose status is unclear is one that is developed as a result of electronic record searches—primarily computer matches, computer profiles, or computer screens. All electronic record searches generate a new file of those who appear in both systems or who meet the criteria of a profile or screen. Agencies argue that the Privacy Act notice procedures would not apply to these because they are only temporary systems that are destroyed in the process of verification, and, therefore, are not record systems under the Privacy Act.

---

[7] Panel on "Privacy Problems Relating to Computer Security," Seventh Annual Symposium on the Freedom of Information and Privacy Acts, sponsored by the Office of Personnel Management's Government Executive Institute, Washington, DC, August 1985.

The second principle of fair information practice is that **there must be a way for an individual to find out what information about him or her is in a record and how it is used.** Technology makes the first requirement of this principle even more important for individuals because more information is being collected from third parties as a result of computerization and on-line searches. While technology could offer individuals more ways to learn what is in their records, OTA found that no agencies have yet offered individuals computer access to their personal information.

Technology has also affected the requirement that there must be a way for an individual to find out how personal information is used. With computerization, the matching of records, searching of files based on profiles, and verifying of information with numerous other record systems have become routine for many record systems. The fact that the uses of information in government databases are increasing does not necessarily mean that individuals will not find out about such uses; however, OTA's research indicates that agencies have generally not informed individuals, at least not in a direct fashion.

The third principle, that **there must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for another purpose without his or her consent,** is affected most dramatically by new applications of technology. The principle includes not just knowledge of the uses of information, but also a means to prevent uses. Given the scale of government recordkeeping and the number of administrative uses of information, it appears to be extremely difficult for an individual to take action.

In computer matching, front-end verification, and computer profiling, information that was collected for one purpose, such as personnel or tax, is being used for another purpose, e.g., detection of fraud, registration for selective service, or payment of child support. In some cases, this principle has been overriden by legislation that has authorized the exchanges. In these instances, the legislative history reveals little explicit consideration of the effect on the fair information principles of the Privacy Act. In the majority of cases, these new uses of information have not been authorized by legislation, but instead have been justified under the routine use exemption of the disclosure provisions in the Privacy Act. This exemption has been used for such a large number of information exchanges and for so many types that it now appears to mean that all uses of Federal records are permitted except those that are expressly prohibited.

The fourth principle of fair information practice is that **there must be a way for an individual to correct or amend a record of identifiable information about him or her.** This principle has become even more important in an age of electronic recordkeeping because more information is collected from parties other than the individual and because information is added to files at indeterminate periods. The increased exchanges and uses of information by Federal agencies make it more difficult to determine what information is maintained and how it is used; therefore it is harder for an individual to correct or amend records. On the other hand, in an age of electronic recordkeeping, it is possible that corrections to individual files could be negotiated via a home computer or agency computer, and agreed upon changes made directly into the system. Based on OTA's research, it appears that no agency is using computers and telecommunications to provide new ways for an individual to amend records.

The fifth principle is that **any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.** It is from this principle that the maxim that information must be accurate, timely, relevant, and complete has been taken [Public Law, 93-579, Sec. 3(e)(5)]. With electronic record systems, data are collected, manipulated, and exchanged much more quickly than in paper systems. The speed of exchanges and large number of users make it more difficult to determine who is responsible for data reliability and use. Once again, the technology offers at least a partial solution in that audit trails can be built into systems. In addition, systems can be programmed to automatically purge records or separate data elements after a specified period of time. OTA found that agencies were not, on the whole, making use of the technology to ensure record quality, and were conducting few reviews of record quality.

Public Opinion.—In general, Americans do not believe that there are adequate safeguards for protecting the privacy of information about people.[8] The percentage of the public believing that personal information about them is being kept in files not known to them has increased from 44 percent in 1974 to 67 percent in 1983. Most Americans, from two-thirds to three-fourths, believe that agencies that release information they gather to other agencies or individuals are seriously invading personal privacy. Yet, a significant percentage of the public believes that public and private organizations do share personal information. Most Americans, 84 percent, believe that master files of personal information could be compiled "fairly easily," and 78 percent would regard this as a violation of their privacy.

There is increasing public support for additional government action to protect privacy. In 1978, two-thirds of the public responded that laws could go a long way to help preserve privacy. Sixty-two percent thought it was very important that there be an independent agency to handle complaints about violations of personal privacy by organizations. In 1982, over 80 percent of the public supported the major principles of the code of fair information principles. In 1983, large majorities of the public supported the enactment of new Federal laws to deal with information abuse, including laws that would require that any information from a computer that might be damaging to people or organizations must be double-checked thoroughly before being used, and laws that would regulate what kind of information about an individual could be combined with other information about the same individual.

---

[8] For a more complete discussion of public opinion and privacy, see ch. 2.

POLICY PROBLEMS

OTA's analysis of Federal agency use of electronic record systems, specifically for computer matching, computer-assisted front-end verification, and computer profiling, revealed a number of common policy problems.

First, **new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves.** As a general principle, the Privacy Act prohibits the use of information for a purpose other than that for which it was collected without the consent of the individual. New computer and telecommunication applications for processing personal information facilitate the use of information for secondary purposes, e.g., use of Federal employee personnel information for locating student loan defaulters, or use of Federal tax information for evaluation of a Medicaid claim.

The expanded use and exchange of personal information have also made it more difficult for individuals to access and amend information about themselves, as provided for in the Privacy Act. In effect, the Privacy Act gave the individual a great deal of responsibility for ensuring that personal information was not misused or incorrect. Technological advances have increased the disparity between this responsibility and the ability of the individual to monitor Federal agency practices. For example, individuals may not be aware that information about them is being used in a computer match or computer profile, unless they monitor the *Federal Register* for notices of such uses or unless questions about their personal information arise as a result of the application. In computer-assisted front-end verification, individuals may be notified on an application form that information they provide will be verified from outside sources, but are unlikely to be told which sources will be contacted.

Additionally, new computer and telecommunication capabilities enable agencies to exchange and manipulate not only discrete records, but entire record systems. At the time the Privacy Act was debated, this capability did not exist. The individual rights and remedies of the act are based on the assumption that agencies were using discrete records. Exchanges and manipulations of entire record systems make it more difficult for an individual to be aware of uses of his or her record, as those uses are generally not of immediate interest to the individual.

Second, **there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with the Privacy Act and related OMB guidelines.** Under the Privacy Act, Federal agencies are required to comply with certain standards and procedures in handling personal information—e.g., that the collection, maintenance, use, or dissemination of any record of identifiable personal information should be for a necessary and lawful purpose; that the information should be current, relevant, and accurate; and that adequate safeguards should be taken to prevent misuse of information.

OMB is assigned responsibility for oversight of agency implementation of the Privacy Act. Prior studies by the Privacy Protection Study Commission (1977), U.S. General Accounting Office (1978), and the House Committee on Government Operations (1975 and 1983) have all found significant deficiencies in OMB's oversight of Privacy Act implementation. For example, under the Privacy Act, information collected for one purpose should not be used for another purpose without the permission of the individual; however, a major exemption to this requirement is if the information is for a "routine use"—one that is compatible with the purpose for which it was collected. Neither Congress nor OMB has offered guidance on what is an appropriate routine use; hence this has become a catch-all exemption permitting a variety of Federal agency information exchanges.

More specifically, OTA found that OMB is not effectively monitoring such basic areas as the quality of Privacy Act records; the protection of Privacy Act records in systems currently or potentially accessible by microcomputers; the cost-effectiveness of computer matching and other record applications; and the level of agency resources devoted to implementation of the Privacy Act. OTA also found that neither OMB nor any other agency or office in the Federal Government is, on a regular basis, collecting or maintaining information on Privacy Act implementation. Given the almost total lack of information on Federal agency personal information activities, OTA conducted its own one-time survey of major Federal agencies and found that:

- the quality (completeness and accuracy) of most Privacy Act record systems is unknown even to the agencies themselves, few (about 13 percent) of the record systems are audited for record quality, and the limited evidence available suggests that quality varies widely;
- even though the Federal inventory of microcomputers has increased from a few thousand in 1980 to over 100,000 in 1985, few agencies (about 8 percent) have revised privacy guidelines with respect to microcomputers;
- few agencies reported doing cost-benefit analyses either before (3 out of 37) or after (4 out of 37) computer matches; authoritative, credible evidence of the cost-effectiveness of computer matching is still lacking; and
- in most Federal agencies the number of staff assigned to Privacy Act implementation is limited; of 100 agency components responding to this question, 33 reported less than 1 person per agency assigned to privacy and 34 reported 1 person.

Additionally, OTA found that there is little or no governmentwide information on or OMB oversight of: 1) the scope and magnitude of computer matching, computerized front-end verification, and computer profiling activities; 2) the quality and appropriateness of the personal information that is being used in these applications; and 3) the results and cost-effectiveness of these applications.

Third, **neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can bé fully debated and resolved.** The efficiency of government programs and investigations is improved by more complete and accurate information about individuals. The societal interest in protecting individual privacy is benefited by standards and protections for the use of personal information. Public policy needs to recognize and address the tension between these two interests.

Since 1974, the primary policy attention with respect to Federal agency administration has shifted away from privacy-related concerns. Interests in management, efficiency, and budget have dominated the executive and legislative agenda in the late 1970s and early 1980s. Congress has authorized information exchanges among agencies in a number of laws, e.g., the Debt Collection Act of 1982 and the Deficit Reduction Act of 1984. In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

A number of executive bodies have been established to make recommendations for improving the management of the Federal Government, e.g., the President's Council on Integrity and Efficiency, the President's Council on Management Improvement, and the Grace Commission. All have endorsed the increased use of applications such as computer matching, front-end verification, and computer profiling in order to detect fraud, waste, and abuse in government programs. However, these bodies have given little explicit consideration to privacy interests. Some executive guidelines remind agencies to consider privacy interests in implementing new programs, but these are not followed up to ensure agency compliance.

In general, decisions to use applications such as computer matching, front-end verification, and computer profiling are being made by program officials as part of their effort to detect fraud, waste, and abuse. Given the emphasis being placed on Federal management and efficiency, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. As a result, ethical decisions about the appropriateness of using certain categories of personal information, such as financial, health, or lifestyle, are often made without the knowledge of or oversight by appropriate agency officials (e.g., Privacy Act officers or inspectors general), OMB, Congress, or the affected individuals.

Fourth, **within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered.** The complexity of Federal Government relations—within executive agencies, between the executive and legislature, between the Federal Government and State governments, and between the Federal Government and the private sector—is mirrored in interconnecting webs of information exchanges. This complexity and interconnectedness is reflected in a myriad of laws and regulations, most of which have been enacted in a piecemeal fashion without consideration of other information policies.

Some of these policies may be perceived as being somewhat inconsistent with others, e.g., the privacy of personal information and public access to government information. Some laws and regulations may only partially address a problem, e.g., Federal privacy legislation does not include policy for the private sector or for the flow of information across national borders. In other instances, issues that are inherently related and interdependent, such as privacy and security, are debated and legislated in separate forums with only passing attention to their relationship.

Additionally, the Federal Government's information systems, as well as its information policy, are dependent on technological and economic developments. Federal funding for research and development and Federal financial and market regulations will have significant implications for these developments. Yet, under the present policymaking system, there is no assurance that these implications will be considered. Likewise, the international information policy environment, as well as international technological and economic developments, affects domestic information policy; yet these factors are not systematically considered in the existing policy arenas.

POLICY ACTIONS

Overall, OTA has concluded that Federal agency use of new information technologies in processing personal information has eroded the protections of the 1974 Privacy Act. Many of the electronic record applications being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered by either the act or subsequent OMB guidelines. Even where applications are covered by statute or executive guidelines, there is little oversight to ensure agency compliance. More importantly, neither Congress nor the executive branch is providing a forum in which the conflicts—between privacy interests and competing interests, such as management efficiency and law enforcement—generated by new applications of information technology can be debated and resolved. Absent such a forum, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

OTA has identified a range of policy actions for congressional consideration, including maintaining the status quo, problem-specific actions, institutional changes, and consideration of a national information policy. These policy actions are discussed below.

Action 1: Maintaining the Status Quo

Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion.

The implication of maintaining the status quo is that the present policy problems and confusion will continue. It is likely that the policy emphasis on management efficiency; on detection and prevention of fraud, waste, and abuse; and on effective law enforcement will continue to take precedence over privacy-related concerns. This emphasis will most likely result in an increased use of current applications of information technology in Federal agencies for record searches such as computer matching, computer-assisted front-end verification, and computer profiling. In addition, it is likely that new applications will be developed.

Without congressional action, individuals will continue to be unaware of the majority of uses and disclosures of personal information by Federal agencies because there will be no notice other than that which appears in the *Federal Register*. If an individual has a question about agency practices and procedures, it is difficult for him or her to find the appropriate person to contact in a Federal agency. If an individual wishes to challenge an agency use of personal information, he or she will not have clearly defined or effective recourse because of the problems with the damage remedies of the Privacy Act.

Additionally, absent congressional action, there will be a lack of information available to Congress and the American people, as well as within agencies, concerning the scale and scope of technological applications applied to records and record systems in Federal agencies. This will make it even more difficult for Congress to be aware of current or proposed agency practices in order to exercise effective oversight. Moreover, the lack of information will aggravate the existing difficulties in monitoring the quality, e.g., accuracy and completeness, of personal information that is used and exchanged by Federal agencies.

If Congress does not address the problems resulting from Federal agency applications of new information technology in processing personal information, then Federal agency staff will be left to interpret the meaning of the fair information principles in an electronic age. This would undermine a primary goal of the Privacy Act because it would increase the discretion of administrative agencies in handling personal information. Additionally, this would not meet the need expressed by some agency staff for more specific guidance from either OMB or Congress.

Most importantly, lack of congressional action will, in effect, represent an endorsement of the creation of a *de facto* national database containing personal information on most Americans, and an endorsement of the use of the social security number as a *de facto* national identifier. Current legislation, such as the Deficit Reduction Act of 1984, has accelerated what had been the gradual development of a national database because of the increased data searches and creation of computerized databases authorized by this legislation. Individual authorizations such as these have been largely unnoticed by the public. However, without consideration of the overall societal and political implications, these authorizations taken together could lead to personal information practices that most of the American public would find unacceptable.

Action 2: Problem-Specific Actions

Congress could also consider a number of problem-specific actions, dealing with computerized record searches, specific categories of information (social security number, tax information, and medical or other sensitive information), microcomputers, and record/data quality.

There are a number of procedural and substantive changes that Congress could legislate. In fashioning such changes, it would be easiest for Congress to deal with specific problem areas. Each of these will be discussed below. These changes are not mutually exclusive. Indeed, to provide the most comprehensive protection for personal information, it may be necessary to legislate in all of these areas.

A. Establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of information, and the rights of individuals.

In order to do this Congress could, in effect, require congressional approval for every record search involving personal information. This would entail amending the "routine use" provision of the Privacy Act to eliminate matching and other record searches from this exemption. As a result, agencies would need to obtain congressional authorization each time they wished to search records containing personal information. Although this approach would enable Congress to monitor record searches and to limit agency discretion in deciding to search records, it may involve a prohibitive time investment for Congress or be a *de facto* prohibition on such searches. Federal agencies likely would be opposed to such an approval process, as they might perceive it as unnecessary interference in internal agency affairs.

Alternatively, Congress could authorize general record searches, but establish explicit standards and procedures. This would require amending the Privacy Act in at least three possible ways:

1. Amend the "routine use" provision to allow record searches under specific circumstances and with specific types of records. In this way, Congress would establish the criteria under which matches and other searches could be done, and the types of records that could not be used in these searches (e.g., medical files or tax and security clearance records).
2. Specify the due process protections (e.g., notice, right to a hearing, right to confidentiality of results, or right to counsel) for persons whose records are to be searched, and the time when due process protections come into effect (e.g., before the match, after the match but before verification, and after verification).
3. Require a cost/benefit analysis before and after every match.

Although establishing standards and procedures may be more workable and realistic than requiring congressional approval for every record search, it does not provide any mechanism to ensure that agencies have complied with the general standards. Based on the experience of agency record searches to date, it appears that oversight and enforcement are essential.

In addition to any of the above amendments, or as an alternative, Congress could require agencies to adopt a 5-year plan for detecting fraud, waste, and abuse. In this way, agency proposals to search record systems would be placed within a context. Agencies would then need to justify record searches as a technique according to criteria such as purpose, cost, and alternatives considered. Such plans could be subject to congressional approval. Again, this would likely be ineffective without critical review, oversight, and enforcement.

Also, in addition to the above, Congress could amend the Privacy Act to require the social security number on all Federal, State, and local government forms. This might improve the accuracy of information used in matching, and might reduce the costs of verifying hits. However, it seems unwise to adopt this action without considering the problems with using the social security number as an authenticator and identifier, and the problem of endorsing a national identifier.

B. *Implement more controls and protections for sensitive categories of personal information, such as medical and insurance.*

Statutes provide specific protection in many areas where personal information is collected and used—e.g., banks, credit agencies, educational institutions, and criminal history repositories. Based on *United States* v. *Miller*, 425 U.S. 435 (1976), if there is no specific statutory basis for an individual's right with respect to a particular type of personal information held by another party, the individual may not be able to assert a claim about how that information is used.

The Privacy Protection Study Commission (PPSC) analyzed the privacy implications of the recordkeeping practices in a number of areas, including insurance, employment, and medical care, and made recommendations for policy. Very few of these recommendations resulted in legislation, although some were embodied in voluntary codes by organizations such as insurance companies and employers.

Medical information is still an area in which an individual's interests are not protected by statute. In 1977, PPSC recommended that "now is the proper time to establish privacy protection safeguards for medical records."[9] The Commission was led to this conclusion by the changing conceptions of the medical record and increased automation. Although many bills to protect medical information have been introduced, none has yet passed. The Federal Government collects, maintains, and discloses a great deal of sensitive medical information. Agencies involved include, for example, the Department of Health and Human Services (HHS), the Occupational Safety and Health Administration, the Environmental Protection Agency, and the Veterans Administration. Agencies collect medical information for purposes such as delivering services, providing cost reimbursements, and conducting research. Legislation could address these and other needs.

Legislating for a specific type of information or specific organizational entity on a piecemeal basis is not without its problems. OTA's research indicates that it is difficult to isolate collection of personal information in this way. Instead, the information infrastructure is complex and constantly overlapping. Needs, interests, and programs converge at many points.

C. *Establish controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government and provide for appropriate enforcement mechanisms.*

---

[9] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, DC: U.S. Government Printing Office, 1977), p. 290.

Agencies appear to be dealing with microcomputer policy on an ad hoc basis. This approach results in variation in the protection afforded personal information by Federal agencies. In establishing policy for the use of microcomputers withing Federal agencies, it is necessary to address the management, data integrity, security, confidentiality, and privacy aspects.

OTA's companion report, *Management, Security, and Congressional Oversight,*[10] analyzes in detail the management, data integrity, and security aspects of information systems policy, including for microcomputers. Briefly, there are four general kinds of measures to protect information systems. First are administrative security measures, such as requiring that employees change passwords every few months; removing the passwords of terminated employees quickly; providing security training programs; storing copies of critical data off-site; developing criteria for sensitivity of data; and providing visible upper management support for security. Second are physical security measures, such as locking up diskettes and/or the room in which microcomputers are located, and key locks for microcomputers, especially those with hard disk drives.

There are also numerous technical measures to assure security, including audit programs that log activity on computer systems; security control systems that allow different layers of access for different sensitivities of data; encrypting data when they are stored or transmitted, or using an encryption code to authenticate electronic transactions; techniques for user identification; and shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment.

Lastly, there are legal remedies to discourage information system abuse, generally known as computer crime, and to prosecute perpetrators. Because computerized information is intangible, its abuses do not fit neatly into existing legal categories, such as fraud, theft, embezzlement, and trespass. This makes computer crime a different kind of criminal act needing special legislative attention. Concern with protecting the privacy of personal information is related to computer crime in that such crimes may involve unauthorized access to personal information.[11]

However, there are important aspects of privacy protection that are not addressed by the security measures discussed above. The Privacy Act establishes individual rights of knowledge, access, and correction, and places requirements on agencies to maintain records in a certain fashion, and to use and disclose records for certain purposes. These procedural and substantive protections are limited to records containing personal information that are "contained in a system of records." A system of records is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [Sec.3(a)(5)]. It is unclear which records maintained on microcomputers come under this definition. Once this has been determined, it will be necessary to provide a means of monitoring these records to ensure that the individual rights of knowledge, access, and correction are provided.

D. *Review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness.*

A central aspect of Federal records policy, as embodied in the Privacy Act and Paperwork Reduction Act, is that records should be complete and accurate. Through the provisions in these acts, Congress has recognized the importance of record quality both to management efficiency and to the protection of individual rights. Agency decisions based on inaccurate or incomplete information can lead to wasteful or even harmful results. Many Federal record systems are now computerized. While computerized systems offer the potential to improve record quality, undetected or uncorrected errors can be disseminated more quickly and widely—with potentially serious consequences.

---

[10] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

[11] For further discussion of computer crime issues and policy options, see ibid., especially ch. 5. Also see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985).

Based on available evidence, including the results of the OTA survey, OTA has concluded that most Federal agencies do not maintain statistics on record quality or conduct audits of record quality. While many agencies have policies and procedures intended to ensure record quality, they do not measure actual quality levels (by comparing record contents with primary information sources), and thus do not have a complete basis for knowing whether or not problems exist.

OTA asked Federal agencies (major components of all 13 cabinet departments plus 20 independent agencies) for the results of any record quality audits conducted on Privacy Act record systems and for record quality statistics on all computerized record systems maintained for law enforcement, investigative, and/or intelligence purposes. Only one agency provided any statistics, and very few of the other agencies indicated that such statistics may exist.

With respect to audits of the quality of Privacy Act records, only 16 of 127 (or 13 percent) agencies responding indicated that they conduct such audits; none provided the results.[12] Only one agency provided record quality statistics (for three systems under its jurisdiction) for law enforcement, investigative, and intelligence record systems. No statistics were provided for any of the other 82 systems reported.[13] Subsequent to the data request, the FBI was asked for and did provide the results of partial audits of the National Crime Information Center (see app. A for further discussion).

Should Congress wish to address the record quality problem directly, the appropriate congressional committees could conduct oversight on Federal electronic record quality, and, if satisfied that a significant problem exists, consider amendments to the Privacy Act and/or Paperwork Reduction Act to provide stronger guidance to the executive branch on this topic. Congress could also ask for General Accounting Office and/or Inspector General audits of record quality of selected Federal agency record systems in order to provide additional independent confirmation of Federal record quality. Finally, Congress could direct one or more of the central agencies responsible for information technology management (Office of Information and Regulatory Affairs, OMB; National Bureau of Standards; or Office of Information Resources Management, General Services Administration) to develop audit packages and techniques that could be used by Federal agencies to measure and monitor record quality.

E. *Review issues concerning use of the social security number as a* de facto *national identifier and, if necessary, restrict its use or legislate a new universal identification number.*

The Privacy Act makes it "unlawful for any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number" unless disclosure is required by law or unless the system of records was in existence prior to January 1, 1975 (the grandfather clause). Although the General Accounting Office, HHS, and numerous task forces all agree that "the social security number is, at best, an imperfect identifier and authenticator,"[14] its use has expanded since 1974. The social security number is an important component in the matching process, and HHS has developed a software program, which will detect erroneous social security numbers, that is to be used in conjunction with a match.

---

[12] A total of 142 agencies were surveyed; 5 did not respond at all, and 10 others responded that the question was not applicable or that the information was not available, for a net total response of 127 agencies.

[13] Again, 142 agencies were surveyed; a total of 85 computerized law enforcement, investigative, or intelligence record systems were identified. Agencies responded as follows: record quality statistics maintained (3 systems); no record quality statistics (63 systems); no response (17 systems); not applicable or information not available (1 system); and classified (1 system).

[14] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, op. cit., p. 609.

Contrary to the stated intent of the Privacy Act, the trend in the use of the social security number appears to be towards its adoption as a *de facto* national identifier. Federal, State, and local agencies, as well as the private sector, have increased their requests, as well as their requirements, for disclosing one's social security number (or Taxpayer Identification Number). In hearings on the Privacy Act, concern with the possibility of the adoption of a universal identifier was voiced. Much of the concern focused on the record searches that a universal identifier would allow. Congress considered setting severe restrictions on the use of the social security number, but was dissuaded by testimony that the costs and implications of such restrictions were unknown. Since enactment of the Privacy Act, Congress has passed numerous laws authorizing Federal agencies to collect the social security number and requiring State agencies to collect it in administering Federal programs.

PPSC was asked to study restrictions on the use of the social security number and to make recommendations. The major finding of PPSC was "that restrictions on the collection and use of the social security number to inhibit exchange beyond those already contained in the law would be costly and cumbersome in the short run, ineffectual in the long run, and would also distract public attention from the need to formulate general policies on record exchanges."[15] PPSC went on to recommend that "the Federal Government not consider taking any action that would foster the development of a standard, universal label for individuals, or a central population register, until such time as significant steps have been taken to implement safeguards and policies regarding permissible uses and disclosures of records about individuals." Such a comprehensive study has not yet been conducted.

If the social security number is being used as a *de facto* standard universal identifier in the United States, both the benefits and hazards of having a national identifier need to be evaluated. The General Accounting Office, PPSC, congressional committees, and the Social Security Administration itself have all discussed parts of these issues. Congress could make a comprehensive review of issues concerning use of the social security number as a *de facto* national identifier and establish a clear policy for the electronic age, with appropriate enforcement mechanisms.

F. Review policy with regard to access to the Internal Revenue Service's information by Federal and State agencies, and policy with regard to the Internal Revenue Service's access to databases maintained by Federal and State agencies, as well as the private sector. If necessary, legislate a policy that more clearly delineates the circumstances under which such access is permitted.

IRS files are valuable sources of information for many record searches because of the variety of information on file (e.g., address, earned income, unearned income, social security number, number of dependents) and because the information is relatively up to date. As a general rule, returns and return information are to remain confidential, as provided for in Section 6103 of the Tax Reform Act of 1976. Under this section, information may be disclosed for tax and audit purposes and proceedings, and for use in criminal investigations if certain procedural safeguards are met.

Additionally, Section 6103(l) allows for the disclosure of tax return information for purposes other than tax administration. The list has grown considerably since 1976, and includes: the Social Security Administration and Railroad Retirement Board (Public Law 94-455, 1976); Federal loan agencies regarding tax delinquent accounts (Public Law 97-365, 1982); the Department of Treasury for use in personnel or claimant representative matters (Public Law 98-369, 1984); Federal, State, and local child support enforcement agencies (Public

---

[15] Ibid., p. 614.

Law 94-455, 1976); and Federal, State, and local agencies administering certain programs under the Social Security Act or Food Stamp Act of 1977 (Public Law 98-369, 1984). Section 2651 of the Deficit Reduction Act also amends Section 6103(l) of the Tax Reform Act and allows information from W-2 forms and unearned income reported on 1099 forms to be divulged to any Federal, State, or local agency administering one of the following programs: Aid to Families With Dependent Children; medical assistance; supplemental security income; unemployment compensation; food stamps; State-administered supplementary payments; and any benefit provided under a State plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Section 6103(m) of the Tax Reform Act also provides for disclosure of taxpayer identity information to a number of agencies, including the National Institute for Occupational Safety and Health and the Secretary of Education.

In all instances, Sections 6103(l) and (m) specify procedures that other parties are to follow in order to gain access to IRS information. Moreover, Federal, State, and local employees outside of IRS who handle IRS information are subject to the same criminal liabilities as IRS employees for misuse or disclosure of the information. The IRS also puts out a publication, *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075; Rev. 7-83), that describes the procedures agencies must follow to ensure adequate protection against unauthorized disclosure.

Pressure to extend the list of agencies that can access IRS information has intensified with interest in record searches to detect fraud, waste, and abuse; to register men for the Selective Service; and for any program that requires a current address for an individual. The IRS's position is that its goal is to maintain a voluntary tax system and that the public's perception that tax information should remain confidential is important to maintaining a voluntary system. Thus, the IRS is, in principle, opposed to disclosing tax information.

Technological advances, however, may make voluntary disclosure of tax information by the affected individual less important and thus reduce the IRS's concern for confidentiality. For example, the IRS is moving towards a system where information provided by the individual would be phased out of the tax return process and replaced with information disclosed directly to the IRS by the sources, e.g., employers, banks, credit agencies, investment companies, mortgage companies, etc. If this becomes the case, the IRS will not need to be concerned with maintaining a voluntary tax system or with protecting the confidentiality of tax information.

Congress may wish to legislate a general, but enforceable, policy regarding the circumstances under which tax information may be disclosed and procedures for such disclosure. The ad hoc process of amending Sections 6103(l) and (m) when the political situation allows, as reflected in the long list of congressionally authorized disclosures, may not be the most effective approach to maintaining the confidentiality of tax information.

Congress may also wish to examine IRS access to other agency and private sector databases, and legislate a more clearly delineated policy for such access. This becomes more important as the IRS relies increasingly on sources of information other than the taxpayer. Additionally, IRS access to other databases may result in inaccurate or irrelevant information being included in IRS records.

Action 3: Institutional Changes

Congress could initiate a number of institutional adjustments, e.g., strengthening the oversight role of OMB, increasing the Privacy Act staff in agencies, or improving congressional organization and procedures for consideration of information privacy issues. These institutional adjustments could be made individually or in concert. Additionally or separately, Congress could initiate a major institutional change, such as establishing a Data Protection or Privacy Board or Commission.

Strengthening the institutional framework for information privacy policy could achieve three purposes, either singly or in combination. First, an institution could play the role of an ombudsman in assisting individuals to resolve individual or class grievances with a Federal agency about personal information practices. Second, it could oversee Federal agency compliance with the Privacy Act and related OMB guidelines. Third, an institution could provide a forum in which proposals to alter personal information practices and systems (e.g., to conduct a computer match or to set up a new computerized database) could be discussed in the context of the implications for personal privacy and consistency with the principles of the Privacy Act.

In the increasingly complex, technological, and bureaucratic environment of the late 1980s, the fair information principles of the Privacy Act are even more important, but the Privacy Act scheme of enforcement and oversight appears to be increasingly anachronistic. For instance, it may not be realistic to ask individuals to control information about themselves in view of the cost and time burdens entailed. Also, the number of organizations that retain personal information is large, and the intricacies of their uses and disclosures of information are such that it appears almost impossible for most individuals to monitor how information is being used.

Moreover, the implicit assumption that each individual has a discrete interest in protecting his or her privacy, and that there is no larger societal interest, can be challenged. Many researchers and practitioners believe that there is also a social interest in maintaining certain boundaries of personal information collection and use. As discussed in chapter 2, the results of public opinion polls implicitly support this view.

There are three weaknesses in a personal information policy that provides for enforcement primarily through individual grievances and requires little direct oversight of agency practices.

First, *the policy relies on individuals to protect their interests*. The Privacy Act requires that individuals be aware of their rights, understand the potential threats posed by Federal agency collection and use of personal information, and be willing to invest the time and money necessary to protect their interests. These requirements place a burden on the individual. Every time one comes in contact with an agency seeking personal information, he or she would need to question the purposes for which information is sought and the necessity of each piece of information.

To ensure that information is not misused, the individual would need to follow up to make sure that no new information was added to the file, and that the uses and disclosures of information were in keeping with the agency's stated purposes. If individuals find that files contain inaccurate or irrelevant information, or that information was used for improper purposes, then they would need to know what legal remedies are available and take action against the Federal agency. Such a procedure means that individuals would need to be conscious of their rights at every stage of the information-handling process. Most people are so accustomed to disclosing information that they rarely think through all of the possible consequences. As Michael Baker suggests:

> What we can expect in the way of self-protective action on the part of individual citizens is severely limited by the fact that record-keeping practices are of relatively low visibility to and salience for the individual.[16]

The second weakness in the enforcement scheme of the Privacy Act is that *it only provides remedies once misuses have been identified*. If an individual has the right to correct inaccurate information or make a case for deleting or amending information in his or her record, the right only "rights" a wrong already committed against the individual. It does not protect the record from further errors or misuses, nor does it prevent similar wrongs from being committed against other individuals. It provides no preventive protection unless the granting of new rights to individuals can be viewed as a means of deterring agencies from engaging in questionable information practices. But the time and money necessary to take action against a Federal agency make it unlikely that many individuals will take advantage of these rights. Thus, the deterrent effect of such rights on agency information practices is likely to be minimal.

---

[16] Michael A. Baker, "Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern," *Columbia Human Rights Law Review*, vol. 4, 1972, p. 89.

The third weakness is that the personal information policy *is not sensitive to the existing imbalance of power between the individual and Federal agencies*. Under the Privacy Act, the interests of individuals are placed in opposition to the needs of the government for information. In most situations, the individual is dependent on the government for employment, credit, insurance, or some other benefit or service. Therefore, the individual is not likely to "afford" the risk of questioning an agency's information practices. Some view this as the most significant policy weakness and argue that:

> [the] enormous imbalance of power between the isolated individual and the great data collection organizations is perfectly obvious: under these conditions, it is a pure illusion to speak of "control." Indeed, the fact of insisting exclusively on means of individual control can in fact be an alibi on the part of a public power wishing to avoid the new problems brought about by the development of enormous personal data files, seeking refuge in an illusory exaltation of the powers of the individual, who will thus find himself alone to run a game in which he can only be the loser.[17]

Strengthening an existing institution or establishing a new one would bring more visibility to the issue of personal information collection and use; provide a central place for individuals to bring complaints and for agencies to seek advice; and enable Congress, the agencies, and the public to get more complete, accurate, and timely information on agencies' practices. The institution could also place limitations on the initial collection of information; review, and possibly approve, proposals to link record systems; and set standards for and oversee data quality in all systems.

A number of institutional changes available to Congress are discussed below:

A. *Strengthen the role of the Office of Management and Budget in the enforcement and oversight of the Privacy Act.*

Under the Privacy Act, OMB is responsible for providing guidelines and regulations, providing assistance to the agencies, overseeing the procedural mechanisms, and preparing the President's Annual Report on Implementation of the Privacy Act. OMB has issued a number of guidelines, most significantly with respect to computer matching and the Debt Collection Act. However, in at least one instance—the guidelines released under the Debt Collection Act—OMB issued its guidelines without time for public comment.[18] In another instance, OMB did not issue guidelines as promised in a judicial action.[19] In addition, OMB has not yet acted on a requirement in the Paperwork Reduction Act to "submit to the President and the Congress legislative proposals to remove inconsistencies in laws and practices involving privacy, confidentiality, and disclosure of information."[20]

From the enactment of the Privacy Act in 1974 until 1980, OMB provided assistance through a separate office with a few staff members within its Information Policy Division. At this time, as the Privacy Protection Study Commission found, "neither OMB nor any of the other agencies with guidance responsibilities have subsequently played an aggressive role in making sure that the agencies are equipped to comply with the act and are, in fact, doing so."[21]

---

[17] S. Rodota, "Privacy and Data Surveillance: Growing Public Concern," *OECD Information Studies #10—Policy Issues in Data Protection and Privacy* (Paris: OECD, 1976), pp. 139-140.

[18] See comments of Christopher DeMuth, Administrator, Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB), and Robert Bedell, Deputy Administrator, OIRA, OMB, in *Oversight of the Privacy Act*, House Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture, 1983, pp. 123-124.

[19] See *Bruce* v. *United States*, 621 F.2d 915 (8th Cir. 1980).

[20] See House Report No. 98-455.

[21] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, op. cit., p. 21.

The Paperwork Reduction Act created the Office of Information and Regulatory Affairs with desk officers to oversee the implementation of information-related policies (including the Privacy Act) within an agency. Although this style of oversight does not necessarily mean that Privacy Act concerns receive less attention, it appears that this has been the practice. Testimony from Christopher DeMuth of OMB at the 1983 hearings on oversight of the Privacy Act[22] indicates (and interviews with OMB confirm) that the desk officers spend little time on Privacy Act matters.

OMB has focused its attention on the review of systems of records, as provided for in the Privacy Act. The act does not offer OMB any other specific guidance and OMB has not taken the initiative—e.g., by reviewing agencies' mechanisms for providing individual access and correction or for maintaining the accuracy of records.

OMB prepares the President's Annual Report on Implementation of the Privacy Act. Annual reports for the years 1975 through 1978 were well-documented studies of agency practices under the Privacy Act, and included descriptions of Federal personal information systems and agency administration, as well as data on use of the access and correction provisions of the act. The information contained in 1980 and 1981 reports was not as complete and focused mainly on systems that agencies designated as exempt from the Privacy Act. In 1982 debates on the Congressional Reports Elimination Act, OMB recommended that the Privacy Act Annual Report be eliminated. Congress rejected this suggestion.[23] The 1982-83 Annual Report on Implementation of the Privacy Act was not delivered to Congress until December 1985. This report synthesized Federal agencies' administration of the act over the past 10 years, and suggested areas for congressional action.

The goal of the Paperwork Reduction Act of 1980 was to reduce paperwork and improve information technology management. The act was designed to coordinate information-related activities of Federal agencies—specifically, automated data processing, telecommunications, office automation, information systems development, data and records management, and, possibly, printing and libraries. The act also acknowledged the importance of information as a resource and made a commitment to the management concept of information resources management, popularly known as IRM.[24]

Concern with protecting the confidentiality and security of personal information and providing individuals access to that information is part of the IRM concept. However, privacy has not been centrally integrated into IRM as presently implemented in Federal agencies. In part, this can be attributed to the fact that the Privacy Act and Paperwork Reduction Act are distinct pieces of legislation, with different public, congressional, and agency constituencies.

Another reason for the lack of integration and coordination is that OMB was somewhat slow to take a lead role in formulating IRM policy. In December 1985, OMB issued Circular A-130, "Management of Federal Information Resources," which sets basic guidelines for the collection, processing, and dissemination of information by Federal agencies, and for the management of information systems and technology. The circular also revised and coordinated existing directives on privacy and computer security. Although the circular succeeds in centralizing information policy in one document, it does not contain any significant changes from previous congressional and OMB policies, and, in general, does not provide detailed guidance to agencies.

In terms of strengthening OMB's role, Congress could to do three things. First, it could amend the Privacy Act, giving OMB the authority to issue regulations—not merely guidelines—and the authority to enforce them. Such additional authority would put OMB in the role of policing agency personal information practices. The advantage of strengthening OMB's authority is that it could be achieved with minor institutional change and minimal overhead. The major disadvantages are that agencies may resist this expansion in OMB's authority, and that continued congressional oversight would be required to ensure that OMB was fulfilling its new responsibilities. Given OMB's prior attention to this area and its other responsibilities, some of which may conflict with data protection/privacy, it may be questionable whether OMB could improve its oversight role even with additional authority.

---

[22] Oversight of the Privacy Act, ibid., pp. 123-124.

[23] See House Report No. 98-455.

[24] For a more complete discussion of IRM, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight*, op. cit.

Second, Congress could enhance OMB's institutional base for dealing with the Privacy Act. This could be done by setting up a separate office with responsibility for data protection/privacy. In order for this office to be effective, Congress would need to ensure that adequate staff and budget are provided. Alternatively, Congress could increase the staff in the Office of Information and Regulatory Affairs and provide a separate staff person per agency who would be responsible for the privacy issues of that agency. Although the institutional framework is in place to achieve these changes quickly, the problem of ensuring OMB's commitment to ensure compliance with the Privacy Act remains.

Third, Congress could upgrade the Office of Information and Regulatory Affairs, possibly by taking it out of OMB and establishing it as a new Office of Federal Management, as provided for in S. 2230, the "Federal Management and Reorganization and Cost Control Act of 1986." This would have the advantage of removing the conflict that exists within OMB between budgetary constraints and management interests. However, it would be important to ensure that privacy be accorded equal importance with other management interests. The principal disadvantage of such a change is that it would be controversial, as it represents a major institutional reorganization.

B. Increase the size, stature, and authority of privacy staff in agencies.

Under the Privacy Act, each agency has designated an official who is responsible for Privacy Act matters. In many agencies, this official is also responsible for the Freedom of Information Act. In most agencies, there is little or no staff support for Privacy Act matters. The OTA survey revealed that 67 percent of agency components responding (67 out of 100) reported one FTE (full-time equivalent) staff person or less assigned to Privacy Act matters. Only 7 percent of agency components (7 out of 100) responding reported having 10 or more FTEs assigned to Privacy Act matters. Five of these components were located in the Department of Justice and included the Drug Enforcement Agency, Immigration and Naturalization Service, Federal Bureau of Investigation, and Criminal Division. The other agencies with more than 10 FTEs assigned to the Privacy Act were the Social Security Administration and the Office of the Secretary in the Department of Commerce.

Congress could amend the Privacy Act to require agencies to provide a certain level of professional and staff support for Privacy Act matters. Such an amendment could provide for adequate training conducted by both related agency staff (e.g., Freedom of Information Act officers, General Counsel staff, staff in the Inspector General's Office, and IRM personnel) and external groups (e.g., OPM's Government Executive Institute and the American Society of Access Professionals).

In amending the Privacy Act, Congress could also specify the responsibilities and authorities of the Privacy Act officers, e.g., to serve as liaison between individuals and agencies in resolution of problems or grievances; to approve, or be consulted about, new record applications; and to maintain information on agency practices. If Privacy Act staff are to be effective in protecting privacy interests from within the agency, their authority must be stated in the legislation; otherwise it is possible that upper management will thwart their efforts.

The primary problem with this action is that enforcement and oversight responsibilities are left within the agencies. Therefore, in addition to statutory changes, intensified congressional oversight of each agency may be required.

C. Improve congressional organization and procedures for consideration of information privacy issues.

At present, Congress does not have a mechanism for coordinated oversight of public laws and bills having privacy implications. Indeed, almost every committee has responsibility for some aspect of the personal information practices of Federal agencies. For example, issues related to the Privacy Act and privacy in general are of interest to the House Committees on Government Operations and on the Judiciary and the Senate Committees on Governmental Affairs and on the Judiciary; privacy issues involving school records are sent to the House Committee on Education and Labor and the Senate Committee on Labor and Human Resources; issues involving privacy of credit records are sent to the Committees on Banking in each House; privacy issues arising under the Freedom of Information Act are considered by the House Committee on Government Operations and the Senate Committee on the Judiciary; issues involving cable subscriber privacy are sent to the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation; in the House, medical records confidentiality has been discussed by the Committees on Government Operations, Energy and Commerce, and Ways and Means, as well as by the Senate Committee on Energy and Commerce; and tax record confidentiality comes under the purview of the House Committee on Ways and Means and the Senate Committee on Finance.

Because of the fragmentation of the committee system and the primacy of substantive concerns in individual committees, privacy interests are often not given thorough consideration. Moreover, it is difficult for interest groups who define their roles as protecting privacy to keep track of relevant legislation and to monitor all pertinent congressional hearings.

If committees with crosscutting privacy jurisdiction were established in both Houses, either as permanent committees, new subcommittees, or select committees, and all bills having privacy implications were referred jointly or sequentially to those committees, privacy issues could be debated and resolved in a more deliberate and focused manner. It is theoretically easy for Congress to make a change of this nature, but politically it is likely to be difficult as reform efforts of the past decade indicate.[25]

An easier alternative would be for Congress to retain the existing committee structure, but provide for better monitoring of bills having information privacy implications, and joint referral of such bills to committees with privacy jurisdiction.

D. Establish a Privacy or Data Protection Board.[26]

The proposal to establish an entity to oversee the personal information practices of Federal agencies is not new. The original Privacy Act that passed the Senate provided for the establishment of a Privacy Protection Commission with powers to:

- monitor and inspect Federal systems and databanks containing information about individuals;
- compile and publish an annual U.S. Information Directory so that citizens and Members of Congress will have an accurate source of up-to-date information about the personal data-handling practices of Federal agencies and the rights, if any, of citizens to challenge the contents of Federal databanks;
- develop model guidelines for implementation of the Privacy Act and assist agencies and industries in the voluntary development of fair information practices;
- investigate and hold hearings on violations of the act, and recommend corrective action to the agencies, Congress, the

---

[25] See, for instance, Steven S. Smith and Christopher J. Deering, *Committees in Congress* (Washington, DC: Congressional Quarterly Inc., 1984).

[26] The term "data protection" is a more precise term for the issues that arise from the collection and use of personal information. It is the term adopted by many European countries. However, privacy is the more easily understood term in the United States.

President, the General Accounting Office, and the Office of Management and Budget;
- investigate and hold hearings on proposals by Federal agencies to create new personal information systems or modify existing systems for the purpose of assisting the agencies, Congress, and the President in their effort to assure that the values of privacy, confidentiality, and due process are adequately safeguarded; and
- make a study of the state of the law governing privacy-invading practices in private databanks and in State, local, and multistate data systems.[27]

The Senate's Privacy Protection Commission was to be composed of five persons who were expert in law, social science, computer technology, civil liberties, business, and State and local government.

A professional staff would have been provided for the commission. The Senate Committee on Government Operations concluded:

> There is an urgent need for a permanent staff of experts within the Federal Government to inform Congress and the public of the data-handling practices of major governmental and private personal information systems.[28]

The Senate considered three alternative institutional placements for the commission—in the U.S. General Accounting Office, in OMB, or in an independent commission—and concluded that an independent commission was, on balance, the best solution. The House did not approve the establishment of a Privacy Protection Commission as it did not see the need for outside oversight of agency practices. As a compromise, both Houses approved the establishment of a Privacy Protection Study Commission to study further the personal information systems and practices of government and private organizations, to make recommendations as to whether the principles of the Privacy Act should be extended beyond Federal agencies, and to make other recommendations as the commission deemed necessary.

The Privacy Protection Study Commission released its report in 1977, and also recommended the establishment of a Federal Privacy Board or some other independent entity with responsibilities similar to those approved by the Senate in 1974. These include the responsibility to: monitor and evaluate the implementation of statutes and regulations; participate in agency proceedings; issue interpretative rules; continue to research, study, and investigate areas of privacy concern; and advise the President, Congress, government agencies, and the States on privacy implications of proposed statutes or regulations.[29]

Since 1977, there have been a number of bills creating a Privacy Commission or Data Protection Board, including H.R. 1721, the "Data Protection Act of 1985," introduced in the 99th Congress. None has received serious congressional attention.

Many Western European countries and Canada have established boards or commissions with responsibilities for the protection of personal information. Because these may serve as a model for such an agency in the United States, descriptions of several countries are found in appendix F.

The advantages and disadvantages of a new privacy authority in the United States would be determined by the design of the agency and the powers with which it is vested. In this respect, a number of policy choices are important.

1. **Whether such an agency should have regulatory authority or advisory authority.** The data protection agencies in Sweden and France are regulatory agencies, with power to determine the personal information systems that government and private sector agencies can create, the information that can be retained, and the parties that can have access to the informa-

---

[27] U.S. Congress, Senate Committee on Government Operations, "Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information," Report No. 93-1183, 93d Cong., 2d sess., 1974, pp. 23-24.

[28] Ibid, p. 24.

[29] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, op cit, p. 37.

tion. The data protection agencies in West Germany and Canada have advisory authority and act as ombudsmen, serving as intermediaries between individuals and agencies, rendering advisory opinions, and lobbying for protection of personal information across a range of policy areas.

In the United States, it is likely that a regulatory agency would be resisted by existing Federal agencies because it would be perceived as having too much control over internal and day-to-day agency affairs. A regulatory agency may also become unwieldy and obstructive. An advisory/ombudsman authority may be more compatible with American philosophical and institutional traditions. It also has a precedent at the State level, e.g., New York. Based on the European and Canadian experience, the advisory/ombudsman model appears to have provided effective oversight of agency practices. Another possibility would be to establish an agency that is primarily advisory, but give it some veto power over particular agency practices.

2. **The institutional placement of such an authority.** The major choice here is whether to make it independent of the executive branch and responsible to the legislature, or to make it part of the executive branch. If it were to be a new office or domestic council within the Executive Office of the President, it could have a great deal of visibility and stature *if* the President decided to make protection of personal information a priority. However, the stature of such a new office might well change with changes in administrations. Also, it could be politicized, especially if budgetary interests were given higher priority or if senior White House officials were interested in using personal information for political purposes—e.g., getting access to IRS information on political opponents or political activists.

Another possibility would be to have the authority established as a bureau within an existing executive department. The advantages of this option would be that it probably would be easier to establish and the overhead costs would be minimal. But, there are significant disadvantages. Inevitably, the power of the new authority would be dependent in part on that of the department, and its character shaped by the department. Additionally, any staff or line department, e.g., the Office of Personnel Management or the Department of Health and Human Services, collects and uses personal information, and, therefore, may have a conflict of interest in the resolution of information collection and disclosure policies.

A third possibility would be to have the authority established as an independent agency of the executive branch. While the agency head presumably would still report to the President, top officials could be made subject to Senate confirmation and even given statutory terms of office. These measures would help protect the authority from inappropriate political pressures and strengthen its institutional independence, as discussed later.

Alternatively, the new authority could report to Congress, either directly or through a special joint committee. The advantage of this approach is that an independent, nonoperating authority would have no stake in the existing personal information exchanges of executive agencies and might be more objective in resolving future conflicts. Moreover, an authority reporting to the legislature would increase the means Congress has to directly oversee the activities of executive agencies. Theoretically, a data protection/privacy authority reporting to the legislature, rather than to the executive, would have independence from the day-to-day operating constraints, as well as the political constraints, of executive agencies.

The disadvantage of having the new agency report to the legislature is that it might be subject to competing political interests, especially if there were different partisan majorities in the two Houses or if the executive and legislature were controlled by different parties. But, even if the authority became politicized, the political maneuverings might be more visible to Congress and the public if the authority reported to Congress than if it were part of the executive. This would seem to ensure a certain degree of accountability.

In determining the placement and powers of a new agency, it will be important to consider the Supreme Court's recent decision in *Immigration and Naturalization Service* v. *Chadha*, 103 S. Ct. 2764 (1983), as well as its pending decision on the constitutionality of the Gramm-Rudman deficit reduction proposal.

3. **The scope of issues for which the agency would be responsible.** Some have proposed that such an authority should be responsible for all privacy issues, e.g., information privacy, surveillance, autonomy/life choices, and "chilling effects" on first amendment rights. If this were the case, information privacy would receive less sustained attention. Also, the size of the authority would, by necessity, be larger. Others have proposed that such an authority should be responsible for all information technology issues, for example, research and development, security, technology transfer, and industrial competitiveness. The same difficulties of focus and size would also apply to an authority with these responsibilities.

The uniqueness and complexity of problems presented by personal information collection and use argue that if an authority is established, it should be solely responsible for personal information issues—not all privacy issues or all information technology issues. However, the growing interrelationships between Federal and State personal information systems, and between public and private systems, argue that, to be effective, an authority would need the power to address all aspects of personal information exchanges. Limiting its purview to Federal agencies could narrow its effectiveness.

4. **Outlining the agency's specific authority and responsibilities.** Generally, such an agency is given some authority to require other agencies to register, or list, their personal information systems, with details on the information held, the sources of information, the uses, the period for which information is retained, and the exchanges and disclosures of information. This process of registration is supposed to ensure that there are no secret systems of personal records. Alternatively, the agency could be given the authority not only to register the systems, but also to approve their existence through a process of licensing. Additional responsibilities that could be considered include:

- some role in settling disputes over issues, such as access and accuracy, that develop between individuals and agencies;
- some role in formally making recommendations on proposed systems or new legislation that have implications for personal information;
- establishing guidelines and standards for specific personal information issues, e.g., what is an acceptable "routine use" or what is "accurate, timely, and complete" information;
- compilation and submission of an annual report on present and anticipated trends in personal information practices; and
- monitoring technological developments and assessing their implications for personal information practices.

5. **Staffing a new authority.** Two models exist for the organization of government agencies. One is to follow the independent regulatory agency model and have multiple commissioners appointed for staggered terms. Another is to have a single head for a fixed term of office. The advantage of the former is that partisan influences are minimized, while the advantage of the latter is that responsibility is clear and visible.

An additional issue is the size of the staff. The maximum number of staff reported for Western European and Canadian counterparts of such an authority is 30. Given the greater population and complexity of Federal/State relations, a somewhat larger staff may be necessary in the United States; however, there are advantages to keeping it small and well organized.

Congress might anticipate two arguments against a proposal to establish a new entity. The first is that it might entail another layer of bureaucracy. However, the purpose of a new entity is to serve as a check on Federal agencies, not to become a part of the bureaucratic establishment. Additionally, the agency could be kept small and its style and organization nonbureaucratic. The second anticipated argument against a new entity would be that the costs associated with privacy protection may increase. This argument may be somewhat specious because, at present, there is no accounting of the costs associated with privacy protection. In calculating these costs, one would need to include agency administrative costs (e.g., the time of Privacy Act Officers, General Counsels, Inspectors General, program managers, and administrative judges); judicial costs (e.g., Department of Justice time and court costs); and the time of individuals.

Action 4: Consideration of a National Information Policy

Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which privacy is a part.

OTA's analysis of Federal agency electronic record systems and individual privacy has confirmed once again the complexity and interrelationships of Federal information policy. The broader social, economic, and political context of information policy is in need of systematic policy study. This discussion could occur in existing executive offices or congressional committees. Alternatively, or in concert, a national study commission could also provide a forum for discussion and examination of a national information policy.

A 1981 OTA study[30] found that there were numerous laws and regulations, some overlapping and some potentially or actually conflicting, that directly and indirectly affect the operators and users of information systems, the consumers of information services, and the subjects of personal information databanks. OTA concluded that continuation of this situation could inhibit many socially desirable applications of information systems or could create even more intractable policy problems in the future. At that time, OTA found that few policymakers were interested in a uniform Federal information policy that would encompass the problems that could arise from the many possible uses of data systems.

OTA identified the need for consideration of an "information policy" that would address the confusing array of laws and regulations—and their strengths, overlaps, contradictions, and deficiencies—within some overall policy framework. This need has not yet been met.

There have been numerous proposals for the establishment of new organizations to study information-related policy problems (see table 15 for a summary).[31] Over the last several years, a growing number of Members of Congress and industry leaders, while not necessarily endorsing specific policies, have expressed concern about the lack of coordinated focus on national information policy issues and the absence of adequate institutional mechanisms. For example:

- Representative George Brown (with Representatives Don Fuqua and Doug Walgren) has introduced legislation to establish an Institute for Information Policy and Research and a Special Assistant to the President for Information Technology and Science Information;[32]
- Senator Sam Nunn (with Senator Frank Lautenberg) has introduced legislation to establish an Information Age Commission;[33]
- Representative Cardiss Collins has introduced legislation to establish a new Office of Telecommunications Policy in the Executive Office of the President;[34]

---

[30] U.S. Congress, Office of Technology Assessment, *Computer-Based National Information Systems*, OTA-CIT-146 (Washington, DC: U.S. Government Printing Office, September 1981)

[31] For a more complete discussion of information policy, see U.S. Congress, Office of Technology Assessment, "Institutional Options For Addressing Information Policy Issues: A Preliminary Framework for Analyzing the Choices," staff memorandum prepared by the Communication and Information Technologies Program, Nov. 29, 1983.

[32] H.R. 744, "Information Science and Technology Act of 1985", 99th Cong., 1st sess.

[33] S. 786, "Information Age Commission Act of 1985", 99th Cong., 1st sess.

[34] H.R. 642, "Telecommunications Policy Coordination Act of 1985", 99th Cong., 1st sess.

Table 15.—Selected Institutional Changes for Information Policy Proposed in the 99th Congress

Proposed institutional change	Problem or issues to which change directed	Organizational form	Functions	Membership	Location	Resources and authority	Duration
Information Age Commission, S. 786 (Nunn and Lautenberg)	Impact of computer and communication systems on society	Commission	Research, policy formulation, and information dissemination	23 members—6 from Congress, 6 from executive branch, and 11 from private sector	Independent—reporting to President and Congress	Hold hearings, negotiate and enter into contracts, and secure cooperation and assistance from other executive agencies	2 years
Office of Federal Management, S. 2230 (Roth)	Management of the Federal Government	Office	Strengthen overall Federal management and, in particular, financial management and information resources management, and reduce the costs of administration	From OMB will be transferred to the Office of Federal Procurement Policy, Office of Information and Regulatory Affairs, and other appropriate functions of OMB. A new Office of Financial Systems will also be established	Executive Office of the President	Provide central policy direction and leadership in general management; maintain oversight of managerial systems and processes; advise President and Congress	Permanent
Office of Critical Trends Analysis, S. 1031 (Gore), H.R. 2690 (Gingrich)	Identification and analysis of critical trends and alternative futures	Office	Publish reports, advise President, establish advisory commission, and promote public discussion	—	Within Executive Office of the President	Legislation requires President to submit report to Congress and requires Joint Economic Committee to prepare report on similar topic	On-going—prepare report every 4 years beginning in 1990
Institute for Information Policy and Research, H.R. 744 (Brown)	Broad range of information policy concerns	Institute	Research, policy formulation, information dissemination, and promotion of innovation	15 member board representing government, industry and commerce, and academic and professional organizations	An independent structure within the executive branch. Director to coordinate with other agencies	—	10 years unless extended by Congress
National Technology Foundation, H.R. 745 (Brown)	High-technology small business, technology transfers, and international activities	Foundation	Analyze and make grants and contracts for development of high-technology small businesses; conduct technology assessments; promote technology transfer and international cooperation	Transfers to the Foundation the following agencies: Patent and Trademark Office, NBS, NTIS, parts of NSF, and other specified agency sections	Independent governmental agency	Award grants, loans, and other assistance, conduct assessments, promote technology transfers	Authorizes appropriations for FY 1986 through FY 1988
Data Protection Board, H.R. 1721 (English)	Personal records held by Federal agencies	Board	Develop guidelines, provide assistance, publish guides, investigate compliance, issue advisory opinions, intervene in agency proceedings	Three members appointed by President with advice and consent of Senate for 7-year terms	Independent executive agency	Conduct inspections, hold hearings, issue subpoenas	Permanent
Department of International Trade and Industry, H.R. 1928 (Watkins)	International trade and industry	Department	Full range including advising, negotiating, and regulating	Travel and Tourism Administration, Patent and Trademark Office, NBS, NTIS, Office of Telecommunications and Information, Office of Small Business Trade Assistance, and Office of Competitive Analysis	Independent department	Legislation requires President, under certain conditions, to submit statement on impact on international economic competitiveness of significant domestic product and service industries	Permanent
Advanced Technology Foundation, H.R. 2374 (LaFalce)	Technology in business, commerce, and industry	Foundation	Promote the commercial application and diffusion of advanced technology within industrial sectors	—	Within executive branch	Create referral service, coordinate programs, provide grants, and develop information management system	Authorizes appropriations through FY 1989

SOURCE: Office of Technology Assessment.

- Representative Glenn English has introduced legislation to establish a Data Protection Board;[35]
- The American Federation of Information Processing Societies has formed a panel of experts on National Information Issues, and the Association of Data Processing Service Organizations has proposed a Temporary National Information Committee.[36]

Most of these proposals view information policy within the context of an information society, i.e., one in which the creation, use, and communication of information will play a central role. There are numerous, interconnected issues arising from the following factors:

- the need to have a greater understanding of the changing role of information and its impact on society;
- the economic and political transition to an information society;
- the effect that the information revolution may have on the governmental process;
- dealing with information as an economic resource, a commodity, and a property;
- the importance of managing information and in trying to assure its accuracy and high quality, especially insofar as it is generated, used, and disseminated by the Federal Government;
- the need to protect individual civil liberties and rights to privacy;
- ensuring access to information and equity that may arise when information is treated more and more as a commodity and less and less as a public good; and
- the enhanced ability of information to travel across national boundaries.

In most discussions of information policy, the relative importance of these issues has not been noted. Indeed, numerous Federal agencies have a role in aspects of information policy, but there is no office or agency providing integration across multiple information policy issue areas. Agencies that might provide such integration, such as the National Telecommunications and Information Administration (in the Department of Commerce) and the Office of Science and Technology Policy (in the Executive Office of the President), have not been provided the necessary mandate and resources, nor do they appear, at least at present, to have the desire to carry out such activities.

Proponents of a national information policy argue that it is just as important as national economic or environmental or defense policy, and deserves a clear focus at the highest levels of government. Beyond this, proponents point to the need for a mechanism to encourage high-level identification and understanding of and leadership on issues arising from the transition to an information society—including issues of protecting individual civil liberties and social equity and the development of information as a valuable economic as well as public good.

Opponents in the past have expressed concern about the dangers of centralizing too much authority over information policy in one place, and have favored continuation of a decentralized policy apparatus with coordination provided through interagency and White House working groups. Some of this concern reflects the experience with the old Office of Telecommunications Policy (created in 1970 in the Executive Office of the President and terminated in 1977). OTP was perceived in part as attempting to influence the content of broadcast news. This raised the specter of a high-level government censorship office.

Realistically, it may be necessary to divide the information problem into more manageable pieces. Because of the urgency of the emerging privacy-related information problems and because there is no inherent group constituency for privacy rights, it may be timely to establish a study commission with responsibility for examination of these interrelated issues.

Two recent proposals for new study commissions in the information policy area include a "National Commission on Communications Security and Privacy" proposed in 1984 by

---

[35] H.R. 1721, "Data Protection Act of 1985", 99th Cong., 1st sess.

[36] AFIPS, *Washington Report*, July 1985, p. 5.

Representative Dan Glickman, of the House Committee on Science and Technology Subcommittee, and the "Information Age Commission" noted earlier. Any national commission on information policy would most likely be broad in scope and encompass many of the issue areas previously identified. A commission established along the lines of these proposals would have a finite lifetime, modest budget, and broad composition (e.g., with representatives from industry, labor, academia, State/local government, and Federal Government). Establishing a new commission need not be a substitute for other congressional policy actions. Indeed, a commission could be viewed as complementing related activities by Federal agencies and could help to improve public understanding of and focus on current and emerging information policy issues.

Appendixes

Appendix A

Update on Computerized Criminal History Record Systems*

Introduction

OTA has carried out an extensive prior study of Federal and State criminal history record systems. The preliminary and final results were published in, respectively, *A Preliminary Assessment of the National Crime Information Center and the Computerized Criminal History System*[1] (1978) and *Assessment of Alternatives for a National Computerized Criminal History System*[2] (1982).

The 1982 study addressed four major areas:

1. the status of criminal history record systems in the United States;
2. the alternatives for a national computerized criminal history (CCH) system;
3. the possible impacts of such a system on the criminal justice process, Federal-State relations, and civil and constitutional rights; and
4. the relevant policy issues that warranted congressional attention to ensure that the beneficial impacts of a national CCH system are maximized and the possible adverse impacts controlled or minimized.

Since 1982, one particular alternative for a national CCH system, known as the Interstate Identification Index (or Triple I), has been tested and generally accepted by the criminal justice community. Triple I is now one of 12 operational files in the National Crime Information Center (NCIC) operated by the Federal Bureau of Investigation (FBI). Triple I is essentially a national electronic index to persons with Federal and/or State criminal history records. The records themselves are maintained in FBI and State record repositories. Triple I replaced the now defunct Computerized Criminal History file on NCIC, and is the largest file on NCIC, as shown in table A-1.

Also since 1982, the extent of computerization in other criminal history record repositories has continued to increase. The FBI's Automated Identification Division System (a CCH record system separate from the NCIC) included 8,740,908 computerized records as of May 1985, compared to about 5.8 million records in October 1981.[3] At the State level, 35 States reported at least a partially computerized criminal history record file as of late 1984, compared to 27 States in August 1982.[4] And 39 States reported, as of late 1984, at least a partially automated name index to persons with criminal history records, as compared with 34 States in August 1982.[5] The fully or partially computerized criminal history files of the States account for an estimated 90 percent of all criminal history record activity.[6]

As discussed in chapter 4 and more extensively in the 1982 OTA report, the Triple I concept evolved after a protracted debate, spanning more than a decade, over the appropriate Federal and State roles in a national CCH system.[7] While the

---

*Outside reviewers for this appendix included Robert R. Belair, Kirkpatrick & Lockhart; Gary R. Cooper, SEARCH Group, Inc.; David F. Nemecek, Federal Bureau of Investigation; and Fred Wynbrandt, California Department of Justice.

[1] U.S. Congress, Office of Technology Assessment, *A Preliminary Assessment of the National Crime Information Center and the Computerized Criminal History System*, OTA-1-80 (Washington, DC: U.S. Government Printing Office, December 1978). Also published as U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure and Subcommittee on the Constitution, *Preliminary Report by the Office of Technology Assessment on the Federal Bureau of Investigation's National Crime Information Center (NCIC) Accompanied by Letters of Comment on the Draft Report*, 95th Cong., 2d sess., December 1978.

[2] U.S. Congress, Office of Technology Assessment, *An Assessment of Alternatives for a National Computerized Criminal History System*, OTA-CIT-161 (Washington, DC: U.S. Government Printing Office, October 1982). Prepared at the request of the House and Senate Committees on the Judiciary, this study was one of four components of the OTA "Assessment of Societal Impacts of National Information Systems." The other components included a September 1981 OTA report on *Computer-Based National Information Systems: Technology and Public Policy Issues*; a March 1982 background paper on *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity*; and an August 1982 OTA report on *Implications of Electronic Mail and Message Systems for the U.S. Postal Service*.

[3] Based on Federal Bureau of Investigation data.

[4] Aug. 6, 1982 data from an OTA survey cited in U.S. Congress, Office of Technology Assessment, *Computerized Criminal History System*, op. cit., pp. 46-48; late 1984 data from a SEARCH Group, Inc., survey cited in U.S. Department of Justice, Bureau of Justice Statistics, "State Criminal Records Repositories," technical report, October 1985, pp. 2-3, prepared by SEARCH Group, Inc., for a Jan. 9, 1986, conference cosponsored by SEARCH Group and the Bureau of Justice Statistics.

[5] Ibid.

[6] OTA previously concluded that, for fiscal year 1981, the 27 States with on-line CCH files accounted for about 85 percent of all criminal fingerprint cards submitted to State and Federal criminal record repositories—a valid measure of criminal history record activity. See OTA, *Computerized Criminal History System*, op. cit., pp. 46-48 and table 5. As of late 1984, eight other States (Louisiana, Montana, New Hampshire, Arizona, Connecticut, Wyoming, Idaho, and Pennsylvania) had automated at least partially, accounting collectively for an estimated additional 5 percent of criminal record activity. Actually, based on 1984 data, those eight States together held about 6.5 percent of the total number of State criminal history records. See Bureau of Justice Statistics, "Criminal Records Repositories," op. cit., p. 2.

[7] Also see U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Patents, Copyrights, and Trademarks, *Computerized Criminal History Records*, hearing, 98th Cong., 1st sess., May 12, 1983; and U.S. General Accounting Office, *Observations on the FBI's Inter-*

Table A-1.—Number of Records Included in NCIC, by File, 1979, 1981, 1985

	Number of records as of		
	June 1981	October 1981	May 1985
Interstate identification index	—	—	9,268,232
Computerized criminal history	1,482,017	1,885,457	—
Stolen securities	1,998,778	2,361,971	2,072,785
Stolen guns	1,337,310	1,674,814	2,052,018
Stolen vehicles	970,714	1,163,771	1,170,613
Stolen articles	1,091,461	1,427,535	1,053,415
Stolen license plates	397,706	543,173	495,225
Wanted persons	148,644	190,159	219,123
Missing persons	21,535	24,610	38,374
Stolen boats	17,615	22,807	24,370
Unidentified persons	—	—	1,067
Canadian warrants	n.a.	183	249
U.S. secret service protective	—	—	91
Total	7,465,780	9,294,327	16,395,662

NOTES: — =file did not exist.
n.a. =data not available.

SOURCE: Federal Bureau of Investigation.

Triple I now appears to be generally accepted by the criminal justice community, OTA reviewed the results of the 1982 study and found that at least three of the key policy issues previously identified have not yet been resolved: 1) noncriminal justice use of criminal history records; 2) the quality (completeness and accuracy) of such records; and 3) policy oversight of the interstate exchange of criminal history information. The status of each is briefly updated below, along with an overview of policy implications.

Noncriminal Justice Use

Criminal record checks are increasingly used in screening applicants for a wide range of jobs and licenses. In the 1982 study, OTA found that noncriminal justice use of criminal history records was already substantial (about one-half of all record requests received by the FBI's Identification Division and about one-seventh of all record requests received by State repositories).

Since 1982, the trend toward criminal record checks for employment and licensing has further intensified. For example, Congress included a provision in Public Law 98-473 requiring that States establish procedures to provide for nationwide criminal history checks for all operators and employees of child-care facilities.[8] There has also been growing interest in implementing criminal record checks for teachers, youth group leaders, and elder-care providers. The primary motivation for the increased emphasis on criminal record checks has been the intensified attention and concern about child abuse (and, to a lesser extent, abuse of the elderly) and the perceived need to more carefully screen applicants for positions entrusted with the care of persons who are likely to be especially vulnerable.[9] In addition, there has been increased emphasis on criminal history record checks for current or prospective Federal employees, especially those in sensitive or classified positions.[10]

Absent policy action, this increasing level of record check activity is likely to aggravate access, equity, and due process problems resulting from the inconsistent Federal and State laws and regulations on dissemination of criminal history records for noncriminal justice purposes. These problems were identified in the 1982 OTA report and further amplified in two 1984 studies commissioned by the FBI to study the implications of using Triple I for noncriminal justice record checks.

One study, conducted by former FBI agent Raymond J. Young and reflecting a Federal perspective, concluded that:[11]

> The most obvious impact (of III) would be the total lack of availability of criminal history record information from States for many or all Federal non-criminal uses. The inability to acquire criminal history data would affect many vital uses, including matters involving national security. . . . In

---

state Identification Index, Report to the Chairman, Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary, Oct. 16, 1984.

[8] U.S. Department of Health and Human Services, *Model Child Care Standards Act—Guidance to States To Prevent Child Abuse in Day Care Facilities*, Washington, DC, January 1985, p. 2.

[9] See, for example, Adrian Higgins, "Day Care Worker Checks Getting Mixed Reviews," *Arlington Journal*, Sept. 6, 1985, p. A7; Linda Lantor, "Fairfax Schools To Tighten Employee Screening," *Arlington Journal*, Sept. 10., 1985, p. A4, and Andee Hochman, "Youth Workers Face Additional Screening; Change Follows Spate of Sex Abuse Cases," *The Washington Post*, Sept. 23, 1985, pp. D1-D2.

[10] See, for example, Mike Causey, "FBI Checks Background of 41,000 at HHS," *The Washington Post*, June 21, 1985, pp. A1-A11; S. 274, the Anti-Nuclear Terrorism Act of 1985, 99th Cong., 1st sess., that would require criminal record checks for nuclear powerplant personnel; S. 1203, 99th Cong., 1st sess., that would allow railroad police and private university or college police access to FBI criminal history records; and S. 1347, the Security Clearance Information Act of 1985, 99th Cong., 1st sess., introduced by Senator Sam Nunn (for himself and Senators William Roth, Lawton Chiles, Albert Gore, and Ted Stevens) and enacted by Congress as Title VIII of Public Law 99-169, that gives the Department of Defense, Office of Personnel Management, and Central Intelligence Agency the statutory authority to access Federal and State criminal history information for national security purposes.

[11] Raymond J. Young, *Federal Non-Criminal Justice Use of the Interstate Identification Index*, prepared for the Federal Bureau of Investigation, Dec. 14, 1984, pp. 5-1, 5-2.

> many other instances, Federal agencies would receive only limited amounts of data from States which, while providing some criminal history information from some Federal uses, place restrictions on the type of criminal history records furnished.

A second study, carried out by SEARCH Group, Inc.—a consortium representing State perspectives—found that:[12]

> [T]here is great disparity among present State laws and policies regarding noncriminal justice access and use. Laws and policies on dissemination range from those in a few States that essentially do not permit access to any criminal history records for any noncriminal justice purpose to those of a few "open record" States that permit access to all or most of such records for anyone for any purpose. Between these extremes is an almost bewildering variety of statutory approaches, with access permitted in particular States to specified records for specified purposes and subject to specified conditions, including requirements that access be authorized by separate legal authority or approved by a council, board, or other official.

As a consequence of these and other as yet unresolved problems, noncriminal justice use of Triple I is currently prohibited.

Record Quality

The importance of accurate records has long been recognized in Federal and State laws and regulations. Since 1970, Congress has explicitly expressed its concern about the completeness and accuracy of criminal history records. Section 524(b) of the Crime Control Act of 1973 required the Law Enforcement Assistance Administration to promulgate regulations that, among other things, were to provide safeguards for the completeness and accuracy of criminal history records. Such regulations were issued in 1975 (as Title 28, Code of Federal Regulations, part 20) and applied to the Federal Government and all States whose criminal history record systems were federally funded in whole or in part.

Federal courts have also ruled on record quality issues. For example, in *Tarlton v. Saxbe* (1974) the U.S. Court of Appeals for the District of Columbia ruled that the FBI had a duty to prevent dissemination of inaccurate arrest and conviction records, and had to take reasonable precautions to prevent inaccuracy and incompleteness. Most States now have statutes or regulations requiring agencies to ensure reasonably complete and accurate criminal history information, including reporting of court dispositions. The number of States with statutes or regulations on record quality increased from 14 in 1974 to 45 in 1979, and to 49 in 1981.[13]

In spite of legislative and judicial mandates to improve record quality, the 1982 OTA study documented significant record quality problems in Federal and State criminal history record systems. The record quality problem that stands out above all others is the lack of information on dispositions. A long series of record quality audits, including OTA's, have shown that, on the average, one-third to one-half of the dispositions that occurred were missing from State and Federal criminal history records.[14] OTA's audits also documented that, for the Federal and State files sampled, roughly one-fifth of criminal history records contained erroneous information.[15]

Since the 1982 OTA report, record quality has received heightened attention. For example, SEARCH Group, Inc.—with Department of Justice (Bureau of Justice Statistics) funding—has held conferences and prepared reports on understanding the problem and on possible solutions, and has developed procedures for conducting record quality audits.[16] The FBI Director has assigned record quality improvement a high priority.[17] And the FBI, with the support of the NCIC Advisory Policy Board, has established an audit team to check State compliance with NCIC procedures, including those on record completeness and accuracy. However, as yet, the audit of record quality is limited to the NCIC files on wanted persons and stolen vehicles, and does not include the criminal history records on which the NCIC Triple I is based.[18]

The FBI has solved part of its record quality problem by terminating the NCIC/CCH file. In effect, it was discontinued as part of the decision to proceed with the Triple I.[19] The FBI has initiated several actions to improve disposition reporting at the Federal level, such as "computer tape exchange with other Federal agencies, automatic generation of disposition follow-up requests, and field recovery teams to review court and agency records," and reports some improvement.[20]

---

[12] SEARCH Group, Inc., *A Study To Identify Criminal Justice Information Law, Policy and Management Practices Needed To Accommodate Access to and Use of III for Noncriminal Justice Purposes*, prepared for the Federal Bureau of Investigation, Sept. 18, 1984, p. 4.

[13] See, U.S. Congress, Office of Technology Assessment, *Computerized Criminal History System*, op. cit., pp. 71-73 and 94-96.

[14] Ibid., pp. 89-96 and 99-102.

[15] Ibid., pp. 89-96.

[16] See SEARCH Group, Inc., *Audit Manual for Criminal History Records Systems*, Sacramento, CA, December 1982; *Audit Documentation Guide: A Model Study Approach*, Sacramento, CA, January 1984; *"SEARCH Audit Clinics Take New Approach" and "National Workshop To Examine Date Quality," Interface*, summer 1984, pp. 19, 31; U.S. Department of Justice, Bureau of Justice Statistics, *Data Quality of Criminal History Records*, prepared by SEARCH Group, Inc., October 1985; and "National Conference on Data Quality and Criminal History Records," Jan. 9-10, 1986, cosponsored by the Bureau of Justice Statistics and SEARCH Group, Inc.

[17] U.S. Department of Justice, Federal Bureau of Investigation, *Minutes of National Crime Information Center Advisory Policy Board*, Washington, DC, Oct. 17-18, 1984, p. 2.

[18] See U.S. Department of Justice, Federal Bureau of Investigation, *National Crime Information Center Control Terminal Audit Manual*, June 4, 1985.

However, audits and surveys of State criminal history record files conducted since 1982 have generally confirmed the results of the 1982 OTA study and suggest significant, continuing record quality problems. For example, 1984 audit results from one State—Illinois—indicated that about 20 percent of arrest events audited had erroneous information and about 50 percent of arrest events audited were missing dispositions, a majority of which were included in local police records.[21] Also, a 1984 national survey of criminal history record quality conducted by SEARCH Group, Inc., found wide variability in disposition reporting. Many States were unable to provide estimates of disposition reporting. For those that did, the average disposition reporting by law enforcement, prosecution, and local correctional agencies was estimated to be about 50 percent—a finding generally consistent with results of other, prior audits.[22] On the positive side, disposition reporting by State correctional agencies was estimated to be about 95 percent. About two-thirds of the States believed that disposition reporting and overall record accuracy were increasing, although most States did not provide hard numbers or audit results to support this belief. States cited increased automation as a major reason for improvement. Other reasons cited include, for example, interagency cooperation, periodic audits, training, reporting laws, and tracking systems.[23]

Policy Advisory and Oversight Body

The 1982 OTA study documented a long history of debate—at least since 1970—over which organization(s) should have a formal policy advisory and oversight role with regard to a national computerized criminal history system. Policy control over any system for the interstate exchange of criminal history information is complicated by several factors:

- the involvement of a wide range of criminal justice agencies--from law enforcement and prosecutorial to judicial and correctional—as providers and users of criminal history information,
- the frequently conflicting Federal and State laws on noncriminal justice access and use,
- the trend towards increasing use of criminal history record checks for employee screening and other noncriminal justice purposes,
- the inevitable tension between Federal and at least some State governments in a sensitive area of interstate activity, and
- the implications of record use for privacy and constitutional rights.

Current policy control over the Triple I is vested in the Attorney General of the United States who has delegated authority to the FBI with a strong advisory role assigned to the NCIC Advisory Policy Board (APB). APB is comprised of 30 representatives:[24]

- 20 law enforcement members elected from the States and localities;
- 6 members appointed by the FBI Director (2 each from the judiciary, prosecutory agencies, and correctional institutions); and
- 4 members appointed by criminal justice associations (1 each by the International Association of Chiefs of Police, National Sheriff's Association, National District Attorney's Association, and National Probation and Parole Association).

However, now that the NCIC/CCH file has been terminated, APB has not defined a clear role for itself with respect to criminal history records beyond the pilot testing and operation of Triple I. The FBI's Identification Division still maintains a large, increasingly computerized criminal history record system, but has no advisory board or council similar to APB. Should an advisory or oversight board be created for criminal history record exchange, either a new board or a modification of APB, membership could encompass groups not currently represented on APB. These could include representatives of, among others, defense attorneys, civil liberties groups, research criminologists (from government or academia), and social scientists concerned with the effects of criminal records on rehabilitation.

---

[19] U.S. Department of Justice, Federal Bureau of Investigation, *NCIC 2000 Project Statement of Work*, Washington, DC, January 1985, p. A-9.

[20] U.S. Department of Justice, *Minutes*, op. cit., p. 226.

[21] Illinois Criminal Justice Information Authority, "Many 'Rap Sheets' Not Automated, Audit Finds," *The Compiler*, vol. 6, No. 2, summer 1985, pp. 3, 8. Also see Bureau of Justice Statistics, *Data Quality*, op. cit. The State of Illinois now has a uniform disposition reporting law and the Criminal Justice Information Authority has prepared an advisory for criminal justice agencies.

[22] Bureau of Justice Statistics, "State Criminal Records," op. cit., p. 4.

[23] Ibid. Also see, for example, improvements in disposition reporting cited in the State of California, per Nov. 18, 1985 memo from Roy T. Iwata, Manager, Disposition Update Section, Record Analysis and Processing Program, Bureau of Criminal Identification.

[24] U.S. Department of Justice, *NCIC 2000*, op. cit., p. A-10.

SEARCH Group, Inc., has, for example, repeatedly taken the position that an advisory body for interstate criminal history record exchange should be more broadly constituted than the present APB. SEARCH Group has stated that the board "be predominantly representative of the States" and that "its representation should ensure that it is responsive to all components of the criminal justice community, not just law enforcement." SEARCH Group also believes that "public interest positions, representing the public at large as well as components of the criminal justice community, must be appropriately represented on the board to ensure that policy decisions are consistent with broad, national considerations."[25]

As long as there is no clear advisory or oversight body for criminal history records exchange, whether APB or some other group, the policy control issue is further complicated by FBI proposals for new intelligence applications of NCIC, for example to include files on white-collar crime and organized crime suspects and associates—as contrasted with the existing wanted persons file, which is limited to persons who have been charged with a crime. These kinds of proposals pose difficult questions. On the one hand, intelligence applications aggravate already existing concerns about record quality and raise new concerns about possible abuse or misuse.[26] On the other hand, the one intelligence file now on NCIC (the Secret Service file) apparently has proved useful, and similar applications may be helpful in other areas.[27]

Policy Implications

The issues discussed above raise the following policy questions:

First, **how should differences between and among State and Federal laws on noncriminal justice criminal history record checks be reconciled?** Presumably, this should be done in a way that reasonably ensures that, for record checks deemed to be lawful and in the public interest, criminal history information will be complete, accurate, and timely. Differences could be reconciled by Federal law, interstate compact, or a set of uniform State laws.[28] Failing any of these, an option would be to use a national full-record file for noncriminal justice purposes, while retaining the Triple I for criminal justice purposes only. A national file maintained by a Federal agency, such as the FBI, would be governed by Federal, not State, laws on record access and dissemination.[29]

Second, **how can record quality be improved?** Independent audits of Federal and State criminal history record files could be required. The existing FBI audit function could be extended to include State and local criminal history records that support Triple I index entries (and related Automated Identification Division System records). An audit function could be assigned to APB or some other advisory body. Congress could enact legislation, along the lines previously proposed by Representative Charles Schumer, that would establish and fund a record quality audit program.[30] Whatever the mechanism, the audits could be conducted so as to produce quantitative estimates of record completeness and accuracy to provide a firm basis for measuring record quality improvement (or lack thereof).

Actually, the current FBI audit process provides a good prototype. As part of the audit function, the FBI audit team selects a statistically valid sample of NCIC entries from the NCIC wanted persons and stolen vehicles files and compares the record contents with State and local source information (e.g., from courts and prosecutors) to determine whether the records are accurate and valid. This FBI record quality audit procedure is similar to that used by OTA as reported in the 1982 study. Indeed, the results of FBI audits of five States indicated that an average of 5.5 percent of the NCIC wanted persons entries were invalid,[31] almost identical to the 5.8 percent result obtained by OTA.[32] The FBI found comparable error rates in the NCIC stolen vehicles files from the same five States.[33] Overall, the FBI audit process appears to be successfully identifying record problems and possible solutions with respect to these two files, and could be extended to include criminal history record files that are relevant to Triple I.

---

[25] SEARCH Group, Inc., policy statement as reprinted in Federal Bureau of Investigation, National Crime Information Center, agenda materials for NCIC Advisory Policy Board meeting, Oct. 17-18, 1984, p. 63.

[26] See, for example, *Privacy Journal*, November 1984, p. 2, and August 1985, pp. 1, 3; Faye A. Silas, "A Bad Rap; Snafus in Computer Warrants," *ABA Journal*, January 1985, pp. 24-25; "Jailing the Wrong Man," *Time*, Feb. 25, 1985, p. 25; Donna Raimondi, "False Arrests Require Police To Monitor Systems Closely," *Computerworld*, Feb. 25, 1985, p. 23; Charles Babcock, "On-line Crime Suspect System Implicated in False Arrest," *Computerworld*, Aug. 19, 1985, p. 12; and John Bennett, "White-Collar Crime File Draws Ire of Left, Right," *Arlington Journal*, Oct. 23, 1985, p. 2. Also see U.S. Congress, House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, *Proposed Contract To Study and Redesign the National Crime Information Center*, Oversight Hearing, 98th Cong., 2d sess., Aug. 1, 1984.

[27] For further discussion, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985), esp. ch. 5 section on "Data Base Surveillance."

[28] See Young, *Federal Non-Criminal Justice Use*, op. cit.; and SEARCH Group, Inc., *Use of III for Noncriminal Justice Purposes*, op. cit.

[29] SEARCH Group, Inc., Ibid., p. 20.

[30] See H.R. 896, Jan. 31, 1985, H.R. 2129, Apr. 18, 1985, and an amendment in the nature of a substitute to H.R. 2129 (discussion draft), Nov. 12, 1985, all entitled the "Criminal Justice Information Improvement Act of 1985," 99th Cong., 1st sess.

Third, **what kind of national policy council or board should oversee the interstate exchange of criminal history records?** Policy oversight issues include, for example: 1) should an advisory policy board have more than advisory power? 2) should the board report to the Attorney General or the FBI Director? 3) should the board have a broader composition when compared to the present APB to reflect the growing noncriminal justice use of criminal history records? 4) should the board include State representatives appointed by the respective Governors rather than, or as a complement to, those elected by law enforcement practitioners? and 5) should a separate board be established with respect to noncriminal justice uses and concerns, while retaining the current APB for criminal justice applications?[34]

One option is to establish statutory guidelines for the role and composition of an advisory body.[35] Another option, not necessarily mutually exclusive, is to assign some oversight responsibilities to any independent Federal data or privacy protection board that might be established (as discussed in ch. 6). One reason that law enforcement and criminal justice record systems were exempted from key provisions of the Privacy Act of 1974 was the expectation at that time that separate criminal justice record privacy legislation would be enacted shortly. One of the legislative proposals at that time, introduced by the late Senator Sam Ervin, Jr., would have established a Federal Information Systems Board. While congressional hearings were held, neither this nor related proposals ever were reported out of committee or voted on by the House or Senate.[36]

---

[31] See Federal Bureau of Investigation, National Crime Information Center Audit Reports for Wisconsin (September 1984), Oregon (October 1984), Arizona (December 1984), Alabama (March 1985), and South Carolina (April 1985).

[32] See U.S. Congress, Office of Technology Assessment, *Computerized Criminal History System*, op. cit., pp. 191-192; also see Kenneth C. Laudon, "Data Quality and Due Process in Large Interorganizational Record Systems," *Communications of the ACM*, vol. 29, No. 1, January 1986, pp. 4-11; David Burnham, "FBI Says 12,000 Faulty Reports On Suspects Are Issued Each Day," *The New York Times*, Aug. 25, 1985; and David Burnham, "Computer Data Faulted in Suit Over Wrongful Arrest," *New York Times*, Jan. 19, 1986.

[33] See FBI NCIC Audit Reports, op. cit.

[34] See OTA, *Computerized Criminal History System*, op. cit., pp. 169-172.

[35] This approach was taken in the original version of H.R. 2129, the Criminal Justice Information Improvement Act of 1985, 99th Cong., 1st sess. A later draft version, dated Nov. 12, 1985, in the nature of a substitute, was limited to record quality matters.

[36] See OTA, *Computerized Criminal History System*, op. cit., pp. 73-74, and S. 2963, the Criminal Justice Information Control and Protection of Privacy Act of 1974, 93d Cong., 2d sess. Also see U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Criminal Justice Data Banks, Hearings*, 93d Cong., 2d sess., March 1974; *Criminal Justice Information and Protection Privacy Act of 1975, Hearings*, 94th Cong., 1st sess., July 15 and 16, 1975; U.S. Congress, House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, *Criminal Justice Information Control and Protection of Privacy Act of 1975; Hearings*, 94th Cong., 1st sess., July 14, 17, and Sept. 5, 1975; and Donald A. Marchand, *The Politics of Privacy, Computers, and Criminal Justice Records* (Arlington, VA: Information Resources Press, 1980).

Appendix B

OTA Federal Agency Data Request

After reviewing all available sources of information on Federal use of information technology, OTA determined that important information was not available in certain areas critical to the OTA assessment. To meet the need for additional information, OTA drafted a request for current agency data covering the areas in which information was lacking or incomplete. The draft request was reviewed by congressional staff of interested committees, and then pretested in four agencies—the Energy Information Administration (Department of Energy), the Food and Nutrition Service (Department of Agriculture), the Office of the Assistant Secretary for Postsecondary Education (Department of Education), and the Veterans Administration. Based on the results of the pretest, the data request was revised. (See attachment 1 for portions of the final, revised data request relevant to this report.)

In April 1985, the data request was sent to the 13 cabinet-level agencies and 20 selected subcabinet agencies (see attachment 2) with a turnaround time of 5 weeks. Sufficient copies were provided for each of the subcomponents of the cabinet agencies. Agencies were informed that no new data collection was to be conducted. An OTA staff member was identified who could be contacted to provide clarification where necessary.

All agencies that were sent the request provided a response, although the responses varied in completeness and quality. A total of 142 agency components provided information. While many of the agencies provided responses well within the time allotted, the completion time for the entire request (142 agency components) was approximately 2 months. The data provided were compiled by OTA staff and appear as appropriate throughout the report.

A draft copy of the OTA report was provided to each of the participating agencies for review and comment.

ATTACHMENT 1

III. Privacy Act (General)

A. Please provide the following data on Privacy Act implementation in your agency:

1. Position and GS level of the Privacy Act Officer or agency official with day-to-day operating authority
2. Position and level of agency official with policy authority
3. Total number of agency staff (in full-time equivalents) assigned to Privacy Act matters
4. Role and responsibility of your agency's Office of Inspector General (e.g., in developing internal agency procedures, responding to Privacy Act requests, preparing Privacy Act materials for OMB).

B. Please specify the procedures your agency follows to ensure Privacy Act record quality, e.g., complete and accurate records. Attach a copy of agency regulations or procedures.

C. Does your agency conduct record quality audits? Yes ___ No ___. If yes, please provide the results of such audits, including copies of any written audit reports.

D. Has your agency developed agency-specific guidelines or procedures for determining what is "relevant" and "timely" information within your agency? Yes ___ No ___. If yes, please provide a copy of such guidelines.

E. Has your agency been a defendant in Privacy Act suits at any time since 1980? Yes ___ No ___. If yes, please list or describe the legal action(s) and basic issue(s) and provide citations.

F. Has your agency revised or updated Privacy Act guidelines with respect to microcomputers? Yes ___ No ___. If yes, please provide a copy of such revised or updated guidelines.

Name ____________________ Agency/Unit ____________________

Title ____________________ Telephone No. ____________________

IV. Privacy Act/Computer Matching and Front-End Verification

A. Has your agency participated in computer matching activities* as a matching agency (the agency performing the match) or as a source agency (the agency disclosing records to the matching agency for use in the match) at any time since 1980? Yes ___ No ___. Please provide a copy of any reports on your matching activities, including the information listed below, to the extent available. Please give priority to information on matches conducted in 1984, with complete quantitative data provided where possible.

1. Date of match
2. Participating parties (indicate source and matching agencies):
    - Federal agencies
    - State agencies
    - Private sector organizations
3. Location of match
4. Frequency of match: one time or ongoing
5. Files matched
6. Method(s) used to exchange records (e.g., direct electronic, computer tape, computer disk)
7. Purpose of match
8. Number of records involved
9. Number of hits
10. Percentage of hits verified

B. Are cost-benefit analyses done prior to computer matching? Yes ___ No ___. If yes, what are the quantitative and qualitative categories used for assessing costs and benefits? How are the cost-benefit analyses used within the agency? Please provide a copy of your agency's three most recent cost-benefit analyses.

C. Do the individual subjects of the match provide written consent prior to a match? Yes ___ No ___. If yes, please attach a copy of the consent form.

D. Are your matches explicitly required or authorized by legislation? Yes ___ No ___. If yes, please list matches required or authorized and cite public law and section for each type of match.

E. Are procedures used to ensure that the subject record files contain accurate information? Yes ___ No ___. If yes, please specify the procedures used.

---

*Defined as the computerized comparison of two or more automated systems of records to identify individuals common to two or more of the record systems or unique to one of the record systems.

F. What is the process once a hit has occurred? What are the standards, procedures, and costs (estimate if necessary) for verification? What is the appeal process, within the agency and outside, for an individual to respond to a "hit"? Have there been any court challenges to the matches? Yes ___ No ___. If yes, what were the results? Please attach case numbers.

G. Are cost-benefit analyses done after matches? Yes ___ No ___. If yes, please provide a copy of your agency's three most recent post-match cost-benefit analyses.

H. Has your agency used computerized front-end verification (i.e., certification of the accuracy and authenticity of information supplied by an applicant by checking against similar information from another agency or source) at any time since 1980 as part of the application process for participation in Federal programs or benefits? Yes ___ No ___. If yes, please provide a copy of any agency reports on your use of front-end verification and describe the process, including use of computers, notice to applicants, and costs. If no, please describe any agency plans for use of front-end verification.

I. What have been the average results of front-end verification as measured by hits (i.e., applicant's eligibility for Federal program or benefit not verified) overall and by Federal program or benefit category. If available, please break down by computerized and manual verifications.

J. Has your agency conducted any cost-benefit studies of front-end verification? Yes ___ No ___. If yes, please provide copies of the three most recent studies.

Name ______________________ Agency/Unit ______________________

Title ______________________ Telephone No. ______________________

V. Privacy Act/Third Party Information and Profiling

A. Does your agency collect any personally-identifiable information in electronic form from third party sources (i.e., from sources other than the subject individual)? Yes ___ No ___. If yes, please provide information on third party collection, including nature of information sources, authority for collection, agency use, procedures to assure accuracy, subject individual's rights to access, review, and challenge the information, and secondary dissemination of third party information outside the agency (specify to whom and for what purpose). If no, please describe any agency plans for collecting third party information.

B. Does your agency use computer-assisted statistical programs and/or related software to develop generic profiles of types or categories of individuals and/or probabilities of such categories of individuals engaging in activities or behavior of interest to the agency (e.g., with respect to misrepresentation of eligibility to receive Federal aid or benefits, non-compliance with or violation of agency regulations, violation of civil or criminal statutes)? Yes ___ No ___. If yes, please provide further details below. If no, please describe any agency plans for the use of such profiling.

C. For each specific use of profiling, please provide the following information, to the extent available:

1. Description of profiling (categories and numbers of individuals, types of behavior)
2. Types of programs and/or software used
3. Development and testing of programs and/or software (please be specific; provide a copy of any written research reports)
4. Source(s) of input data
5. Authority for the profiling (cite specific statute or regulation where applicable)
6. Agency use of the profiling
7. Results of agency use of the profiling (e.g., percentage of hits on targeted individuals, civil and/or criminal penalties imposed). Please provide a copy of any profiling evaluation reports.

Name ______________________ Agency/Unit ______________________

Title ______________________ Telephone No.______________________

VI. Privacy Act/Debt Collection Act

A. Does your agency report or refer delinquent and/or nondelinquent commercial and/or consumer (individual) debts to private sector credit bureaus? Yes ___ No ___. If yes, please provide further details below. If no, please describe any agency plans for the use of private sector credit agencies.

B. For each specific type of debt referred to private sector credit bureaus, please provide the following information, to the extent available:

1. Description of type of debt referred
2. Format of referral (e.g., paper, microfiche, computer tape, direct electronic)
3. Procedures/agreements between the agency and credit bureau with regard to:
    - o security
    - o record quality (completeness and accuracy)
    - o secondary dissemination
    - o subject individual's or organization's access, review, and challenge rights
4. Number and type of complaints received from debtors referred to private sector credit bureaus, and resolution of those complaints
5. Results of debt referrals by type of debt (e.g., dollars recovered and as percentage of debt referred)

C. Does your agency use private sector credit reports in making agency decisions about eligibility for Federal programs and benefits? Yes ___ No ___. If yes, please provide details on the specific purposes of such use (e.g., when awarding loans, contracts, grants).

Name ______________________ Agency/Unit ______________________

Title ______________________ Telephone No. ______________________

VII. Privacy Act/Electronic Records Management and Electronic Mail

A. Please estimate, to the extent possible, the number and percentage of manual versus computerized records maintained by your agency in the following categories for fiscal years 1975 and 1984:

		Manual		Computerized		Total	
		No.	%	No.	%	No.	%
Records subject to Privacy Act	1975	___	___	___	___	___	___
	1984	___	___	___	___	___	___
Other records maintained subject to public law or agency regulation	1975	___	___	___	___	___	___
	1984	___	___	___	___	___	___

B. If your agency maintains one or more record systems subject to the Privacy Act, please list the 10 largest Privacy Act record systems, the total number of persons and records in each system, and the percentage of manual versus computerized records for each system.

	Record System	No. Persons	No. Records	%Manual	%Computerized
1.	___	___	___	___%	___%
2.	___	___	___	___	___
3.	___	___	___	___	___
4.	___	___	___	___	___
5.	___	___	___	___	___
6.	___	___	___	___	___
7.	___	___	___	___	___
8.	___	___	___	___	___
9.	___	___	___	___	___
10.	___	___	___	___	___

C. For your agency's computerized records (e.g., records stored in electronic form on computer tape or disk), please provide the following information, to the extent available:

1. Procedures for backup copies (please estimate percentage of records backed up by each of the following: paper copy, microfiche or microform, duplicate computer tape or disk, no backup, more than one backup)

2. Procedures for storage and maintenance of electronic records (please specify how long such records are stored, what protections are used to protect against alteration, and when and how electronic records are archived, i.e., moved off premises to a remote storage location)

3. Procedures for purging of electronic records (under what conditions and when are records purged, i.e., eliminated or destroyed)

4. Procedures for verification of signatures on or authenticity of electronic records

5. Procedures for duplication or copying of electronic records (e.g., what is the agency definition of "record copy" of an electronic record)

D. Does your agency use electronic mail? Yes ___ No ___. If yes, please provide further details below. If no, please describe any agency plans for use of electronic mail not otherwise described in response to Section I.

E. Please provide the following information, to the extent available, on your agency's use of electronic mail.

1. Total volume in number of messages sent (i.e., pieces of electronic mail) per year for fiscal year 1984
2. Type of electronic mail system used (e.g., in-house, outside contractor, commercial)
3. Total volume in number of messages received per year for 1984
4. Content of messages sent (in percentage of 1984 total):

Purpose	Percentage
Intra-agency correspondence/memos	_____%
Intra-agency records/reports	_____
Interagency correspondence/memos	_____
Interagency records/reports	_____
External correspondence/memos	_____
External records/reports	_____

5. How long are backup message copies retained in electronic and/or paper form?

6. Who participates in electronic mail? (Specify type of agency staff, e.g., administrative, secretarial, technical, research)

F. Does your agency have a set of privacy/confidentiality/security practices or policies developed specifically for electronic mail? Yes ___ No ___. If yes, please provide a copy or describe in detail.

Name ______________________ Agency/Unit ______________________

Title ______________________ Telephone No. ______________________

VIII. Investigative, Law Enforcement, and Intelligence Applications

A. Does your agency maintain computerized record systems for investigative, law enforcement, and/or intelligence purposes? Yes ___. No ___. If yes, please provide the detailed information below.

B. For each such computerized record system, please provide the following information, to the extent available:

1. Name of record system
2. Purpose of record system
3. Number of records
4. Number of persons
5. Types of record information (e.g., individual names, social security number, address)
6. Sources of record information
7. Users of record systems and rules on access
8. Statistics on quality of records and procedures for maintaining record completeness and accuracy

C. Does your agency use computer-assisted statistical programs and software to develop profiles of types or categories of individuals engaging or likely to engage in activities of investigative, law enforcement, and/or intelligence interest to your agency? Yes ___. No ___. If yes, please provide further details below. If no, please describe any agency plans for the use of such profiling.

D. For each specific use of computer-based profiling, please provide the following information, to the extent available (and not otherwise provided in Section V):

1. Description of profiling (categories and number of individuals, types of behavior)
2. Types of programs and/or software used
3. Development and testing of programs and/or software (please be specific; provide a copy of any written research reports)
4. Sources(s) of input data
5. Authority for the profiling (cite specific statute or regulation where applicable)
6. Agency use of the profiling
7. Results of agency use of the profiling (e.g., percentage of hits on targeted individuals, civil and/or criminal penalties imposed). Please provide a copy of any profiling evaluation reports.

Attachment 2.—Federal Departments and Agencies Responding to OTA Data Request

Cabinet department	*Number of agency components responding*
Agriculture	25
Commerce	17
Defense	14
Education (agencywide)	2
Energy (EIA, FERC, and rest of agency)	3
Health and Human Services	9
Housing and Urban Development (agencywide)	1
Interior	9
Justice	13
Labor	8
State (agencywide)	1
Transportation	11
Treasury	9
Subtotal	122
Independent agencies	
Commission on Civil Rights	1
Consumer Product Safety Commission	1
Environmental Protection Agency	1
Equal Employment Opportunity Commission	1
Federal Communications Commission	1
Federal Elections Commission	1
Federal Emergency Management Agency	1
Federal Reserve System	1
Federal Trade Commission	1
General Services Administration	1
National Aeronautics and Space Administration	1
National Archives and Records Administration	1
Nuclear Regulatory Commission	1
Securities and Exchange Commission	1
Selective Service System	1
Small Business Administration	1
Arms Control and Disarmament Agency	1
U.S. Information Agency	1
Agency for International Development	1
Veterans Administration	1
Subtotal	20
Total	142

Appendix C

List of Contractor Reports

Copies of the following contractor reports completed in support of this assessment will be available in late 1986 from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161, (703) 487-4650.

1. William H. Dutton and Robert G. Meadow, *Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties, and the Democratic Process*, Annenberg School of Communications, University of Southern California, prepared for OTA, January 1985.
2. David Flaherty, *Data Protection and Privacy: Comparative Policies*, prepared for OTA by The Privacy Project, University of Western Ontario, Jan. 8, 1985.
3. Karen B. Levitan, Patricia D. Barth, and Diane Griffin Shook, *Agency Profiles of Civil Liberties Practices*, prepared for OTA by The KBL Group, Inc., Dec. 28, 1984.
4. Robert Ellis Smith, *Report on Data Protection and Privacy in Seven Selected States*, prepared for OTA, Feb. 15, 1985.

Appendix D

Other Reviewers and Contributors

Ralph W. Adams
National Security Agency

Patricia Aronsson
National Archives and Records Administration

William L. Ball
U.S. Department of State

Robert P. Bedell
Office of Management and Budget

Jane Bortnick
Congressional Research Service

Frank G. Burke
Acting Archivist of the United States

Richard Ehlke
Congressional Research Service

Kenneth R. Erney
U.S. Department of State

Liz Handley
U.S. Department of Health and Human Services

Mary C. Lawton
U.S. Department of Justice

Fred Lothrop
PSC, Inc.

Gary Marx
Massachusetts Institute of Technology

Francis A. McDonough
U.S. General Services Administration

Sandra Milevski
Congressional Research Service

Oscar W. Mueller, Jr.
U.S. Department of the Interior

David Mullins
U.S. General Services Administration

Dale Nesbary
National Conference of State Legislatures

Hugh O'Neill
Formerly U.S. Department of Health and Human Services

Ronald S. Plesser
Blum, Nash & Railsback

Edward J. Regan
Manufacturers Hanover Trust Co.

Nancy Reichman
University of Denver

Harold Relyea
Congressional Research Service

David N. Richardson
Yankelovich, Skelly & White, Inc.

Alice Robbin
University of Wisconsin, Madison

Roger K. Salaman
National Telecommunications and Information Administration
U.S. Department of Commerce

Gail Shelton
U.S. Department of Health and Human Services

Ollie R. Smoot
Computer & Business Equipment Manufacturers Association

Appendix E

Summary of Final Rules for Income and Eligibility Verification Required Under the Deficit Reduction Act of 1984*

The Departments of Agriculture, Labor, and Health and Human Services issued final rules in the *Federal Register* on February 28, 1986, to implement Section 2651 of the Deficit Reduction Act of 1984 (DEFRA). Section 2651 amended the Social Security Act, the Food Stamp Act, and the Internal Revenue Code to require federally funded public assistance and unemployment agencies to improve the accuracy of eligibility determinations and benefit programs by exchanging information with each other and by obtaining unearned income data from the Internal Revenue Service (IRS) and other income and wage data from the Social Security Administration (SSA) and from State wage and Unemployment Insurance Benefit (UIB) data files. The rules require State agencies to develop an Income and Eligibility Verification System (IEVS) for administering the following programs:

1. The Food Stamp Program under the Food Stamp Act of 1977, as amended.
2. The Aid to Families With Dependent Children (AFDC) Program under Title IV-A of the Social Security Act; the Adult Assistance Programs under Titles I, X, XIV, and XVI of the Social Security Act.
3. The Medicaid Program under Title XIX of the Social Security Act.
4. The Unemployment Compensation Program under Title III of the Social Security Act.

Use of IEVS Data.—IEVS data can be used to obtain information for prosecutions, i.e., as the basis for investigations in the same way as it is used as a basis of inquiry about household circumstances.

Oversight and Coordination of IEVS.—No specified type of oversight requirement on States; no statutory requirement on States to organize implementation of IEVS in any special or uniform way; no plan to add to existing Federal oversight mechanisms; not feasible, within established timeframes, to establish uniform guidelines and programming specifications for the required matches.

Access and Use of Information.—Data must be requested from all of the required sources on applicants for Medicaid, AFDC, adult assistance, and food stamp programs at the first available opportunity, which would be the next scheduled match for each source. The State Wage Information Collection Agency (SWICA) and the State Unemployment Compensation Agency must accept and process requests for wage information at least twice a month. Requests for IRS data for applicants must be made at the first available monthly IRS match date. With regard to requesting data from SSA, at the first available opportunity, the applicant should be processed in the next cycle of the Beneficiary and Earnings Data Exchange (BENDEX) System or queried through the Third Party Query (TPQY) System.

Timeframes.—Proposed rules required that IEVS information be used to determine eligibility within 20 calendar days of receipt. Final rules extended this to 30 days because of the need to verify IEVS information.

Cost Effectiveness.—". . . all of the required information sources have been demonstrated to be useful in preventing incorrect eligibility and benefit amounts, either by directly offsetting costs or by helping deter nonreporting by applicants and recipients" (p. 7183).

Automation.—"We encourage States to develop on-line systems and other methods for rapid turnaround of State agency requests so that wage and UIB data can be used to determine eligibility and benefits of applicants" (p. 7180). "We encourage the use of on-line systems for front-end verification, but our rules do not require States to have this capability" (p. 7181). "SSA and IRS have not found it cost effective to make the wage and self-employment (SSA) and unearned income (IRS) information accessible on-line for their own agency purposes. Therefore, it would not be feasible to allow States on-line access to these files. SSA has the capability of providing on-line access to bene-

---

*The final rules appeared in the *Federal Register* on Feb. 28, 1986 (vol. 51, No. 40, pp. 7178-7217). The proposed rules were published in the *Federal Register* on Mar. 14, 1985 (50 FR 10450). Comments on the proposed rules were received from 53 parties: 38 States, 6 client advocate groups, 4 local or county welfare agencies, 4 Federal agencies, and 1 private citizen.

fit data. A pilot project is being conducted with Tennessee to provide wire-to-wire exchange of benefit data" (p. 7184).

In the proposed rules, it was stated that "the statutory requirements for IEVS mandated a logical process and not necessarily a physical or automated system to assure the timely and efficient exchange of information among the various programs." It was recognized that "an increasing number of States are operating automated on-line systems to exchange, maintain and make data available to workers," but this level of automation was not required. Many commenters suggested that automation would be required to meet IEVS requirements fully. The Federal agencies agreed that "automating the required IEVS functions would enhance a State agency's ability to respond in a timely fashion to the substantial amount of information made available to the State agencies as a consequence of the data exchange requirements," but did not believe that such automation should be required in the rules (p. 7194).

State Wage Information Collection Agencies.—Final rules retain requirement for quarterly wage matching. Employers in each State are required to report wages quarterly.

Unemployment Insurance Benefits.—Agencies are required to do data matches for UIB information at application and for 3 months following application or loss of employment. For the Food Stamp Program, in addition to wage and UIB information, State agencies are required to request and utilize any information available from Unemployment Compensation (UC) agencies to the extent permitted.

Internal Revenue Service.—An annual match of recipients against IRS data on unearned income is required. IRS has scheduled 11 monthly runs of State tapes against its national file of unearned income information. IRS will only process one tape per month per State.

Social Security Administration.—State agencies are required to access all available SSA data on applicants by using the TPQY system (for SSA benefit data) or the BENDEX System (for pension, earnings, and self-employment information). If TPQY is used, when the applicant becomes a recipient the State agency must add the name to BENDEX. Regarding data quality, the final rules emphasize two factors: 1) except for UC and SSA benefit data, the information obtained through IEVS will be generally treated as a lead for further verification activity, for example, SSA earnings will almost always need to be verified; and 2) "if a State receives what they believe [sic] is incorrect information, no adverse action should be initiated until the discrepancy is resolved" (p. 7186).

Interprogram and Interstate Exchange.—All programs in IEVS are required to exchange income and eligibility information with each other in accordance with interstate and intrastate agreements in effect and as appropriate to the requesting program's verification and eligibility determination needs. State agencies are encouraged to request data from adjacent jurisdictions and other States where experience indicates the data would be useful. States may also access the State Employment Security Internet System for IEVS matches, although this is not a requirement. The Internet System is still under development and its potential uses are still being evaluated by the Department of Labor.

Alternate Sources.—A State agency may obtain data from sources other than those specified in the regulations (from banks, for example) if it can demonstrate to the respective Secretaries that the alternate source furnishes data as timely, complete, and useful as data from the source specified in the regulations.

Independent Verification.—Independent verification is an inquiry about a possible discrepancy in the information reported by the individual and information reported from other sources. Information can be independently verified by contacting the applicant or a third-party source (for example, the employer or bank that reported the information). "The option of contacting a third party is necessary in cases where the recipient fails or refuses to cooperate, the State agency believes it to be in the interest of the investigation of potential fraud or when other factors indicate that a third party contact is preferable" (p. 7188).

DEFRA requires independent verification of IRS unearned income. With respect to other information obtained through IEVS, the food stamp program set explicit guidelines for verification, while the AFDC, adult assistance, and Medicaid programs require independent verification of IEVS information if determined appropriate based on agency experience. "The State agencies remain responsible for ensuring that any information they use in determining eligibility and payment amounts is correct" (p. 7196).

Social Security Numbers: Furnishing, Using, and Verifying.—DEFRA requires each applicant for, and each recipient of, AFDC, adult assistance in the territories, food stamps, unemployment compensation, and Medicaid to furnish his or her social security number in order to associate information on applicants and recipients for the required matches. Existing AFDC and food stamp program rules already require the furnishing of social security numbers. All State agencies implementing Medicaid, AFDC, food stamp, and adult assistance programs must verify applicant and recipient social security numbers to ensure efficient administration of the matching programs and to prevent improper disclosure of information. However, eligibility determinations cannot be delayed pending social security number verification.

Social security numbers can be verified through the BENDEX, State Data Exchange (SDX), TPQY, and social security number verification systems. There is no required order for using these systems. SSA generally verifies the social security numbers of recipients of title II or title XVI benefits. Therefore, a social security number for such an individual received through BENDEX can be considered verified. However, not all social security numbers in BENDEX are verified. At present, the social security number verification system is being redesigned, and when completed, verification of social security numbers should be completed within 3 weeks. On-line access to the social security number verification system is not feasible at this time. SSA is working on a pilot project with Tennessee to provide wire-to-wire exchange of benefit data, including verification of social security numbers. SSA expects to offer the same service to other States.

Routine Notice to Individuals.—DEFRA requires that all applicants and recipients be notified that information available through IEVS will be requested and utilized. Notification is to be given at application and periodically thereafter, i.e., based on existing program case-processing cycles. Notice must be written and must inform the individual that income and eligibility information may be obtained using his or her social security number and will be used in determining eligibility. The notice must include the types of agencies that will be contacted, for example, unemployment compensation agencies.

The Departments of Labor, Agriculture, and Health and Human Services "believe that State agencies should obtain assurances from provider agencies that their automatic data processing methods prevent providers from recording what recipient names and/or social security numbers are processed and that individuals having access to such information are bound by the disclosure rules of the various programs" (p. 7191).

Notice of Expiration or Adverse Action.—Under the proposed rules, the applicant or recipient had to be notified of any planned adverse action and had to be given the opportunity for a fair hearing. The food stamp program proposed rules also included a provision under which households that failed to respond in a timely fashion to State agency requests for information would be sent a notice of expiration of their certification period. The final rule replaces the proposed use of the notice of expiration with a notice of adverse actions when a household does not respond in a timely fashion to a State agency inquiry about IEVS information.

Safeguards for Confidentiality.—DEFRA requires each State agency to institute adequate safeguards to assure: "(1) that information is made available only to the extent necessary to assist in the valid administrative needs of the program receiving the information and that unearned income data from IRS is exchanged only with those agencies authorized to receive it; and (2) the information is adequately protected against unauthorized disclosure for other purposes" (p. 7192).

Oversight.—DEFRA did not mandate any reporting system to gather information on actions taken and savings realized. The proposed rules asked for comments on such a system. In the final rules, the Departments of Agriculture, Labor, and Health and Human Services stated that reporting "is necessary to help ensure the proper and efficient administration of the programs," and that they were "developing uniform, annual reporting requirements intended to minimize the recordkeeping and reporting costs and burden on States, while enabling the Federal Government to monitor compliance with the requirements for accessing and using information" (p. 7197).

Appendix F

Privacy and Data Protection Policy in Selected Foreign Countries[1]

Many Western European countries and Canada have also established policy to protect the collection and use of personal information. Many of these countries have created boards or commissions with responsibilities for overseeing government and private sector information practices, and acting as ombudsmen for individuals. Because the policies of these countries may serve as a model for policy actions in the United States, descriptions of the policies of several countries follow.

The Federal Republic of Germany

The Federal Data Protection Act became law on January 27, 1977. Its provisions apply to both computerized and manual personal information systems in both the public and private sectors. Registration of all private and computerized public information systems is required under the act. Although the general principles regarding rights of individuals and restrictions on the collection and use of personal information are the same for public and private organizations, the methods of regulating the two sectors differ.

The act provides for the appointment of a Federal Commissioner for Data Protection to supervise public sector information systems. This position was added to the draft legislation at the insistence of the West German legislature; the original government bill did not call for such an official. The Commissioner, who serves for a 5-year term and may be reappointed once, has the authority to investigate complaints, inspect information systems, require information from agencies, and make recommendations. The Commissioner does not have licensing power. Nor does the office have enforcement powers; rather, the head of each public agency is responsible for ensuring compliance by the agency. The Commissioner serves, therefore, in an advisory capacity rather than a regulatory one. Up to now, the advice of the Commissioner has been taken seriously by the Federal agencies, including the national security agencies and the Federal police. In essence, it has not been politically viable for the heads of Federal agencies to ignore the Commissioner's advice, which is normally given privately at first and later as part of a process of negotiation over competing interests in the use of information. The Federal Commissioner for Data Protection is subject to supervision by the government and reports to both the Minister of the Interior and to Parliament.

Private organizations maintaining personal information systems are supervised by the Land (State) authorities to which the organization belongs. For example, the Land authority that regulates banking activity is now responsible for ensuring that the banks also comply with data protection rules.

Sweden

Sweden was the first country to pass national legislation regarding the collection and use of personal information. The purpose of the 1973 Data Act was to protect the confidentiality of records, to rationalize the personal information policies of organizations, and to expand individual rights and state protection to private information systems. The Data Act covers all computerized personal information systems in the public and private sectors. It established a regulatory agency, the Data Inspection Board (DIB), which is independent of the government and has the responsibility for licensing all automated personal information systems in both the public and private sectors. The 1973 statute mandated DIB licensing in advance, but a more permissive and somewhat less bureaucratic system, focusing more on sensitive uses of personal information, was introduced in the 1982 revision. The revised law was designed to reduce the bureaucratic burden of data protection and to make the system of selective licensing of personal information systems self-supporting. These revisions occurred in response to DIB's own internal assessment of what changes were necessary and the government's general desire to reduce the costs of government. It is noteworthy that, because of Opposition fears of appearing to weaken data protection, the 1982 amendments passed by only one vote.

The Data Inspection Board has a Board of Directors, appointed for fixed terms, representing various political parties and interest groups, and a staff of less than 30. DIB exercises a great deal of power. It has the authority to control the collection and dissemination of personal data, to regulate the usages of the resulting register, and to set up a system of responsible keepers for computerized databanks. DIB also has the powers to investigate complaints, to inspect information systems, and to require information from organizations. The power of the cabinet or legislature to create a personal file outside the jurisdiction of DIB is an example of several safety valves in the legislation that prevent DIB from acting in a discretionary fashion on any specific measure.

---

[1] Material for this section was derived from David H. Flaherty, "Data Protection and Privacy: Comparative Policies," OTA contractor report, January 1985.

The Data Act contains a few general data protection rules, for example, the data subject's right of access and right to challenge are guaranteed in the act. But, DIB is responsible for designing detailed rules for particular systems and users, including what information may be collected, and the uses and disclosures of this information.

France

The 1978 Law on Informatics, Data Banks, and Freedoms is an expansive and innovative statute. Article 1 well illustrates this point:

> Informatics ought to be at the service of each citizen. Its development should occur in the context of international cooperation. It ought not to threaten human identity, the rights of man, private life, nor individual or public freedoms.

The 1978 law created an independent administrative agency with regulatory power, the National Commission on Informatics and Freedoms (CNIL). It is the first administrative agency in France with statutory independence from the government. CNIL is obliged to ensure the observance of the 1978 law and to make decisions on the authorization of particular information systems in response to requests. The Commission has 17 part-time members chosen for 5-year terms by various official government bodies, including the Senate, the National Assembly, the Council of State, the Court of Cessation, and the Court of Financial Accounts. There are also data protection officials in each government agency.

Critics argue that CNIL has never taken a tough decision against the government with respect to a proposed new personal information system. CNIL has rarely turned down a government proposal; it tends to negotiate changes during the process of application for approval. Because of the way it works in responding to specific requests for advice or licenses, CNIL has not yet reviewed in detail all of the databanks that existed prior to the enactment of the 1978 law.

United Kingdom

The Data Protection Act became law on July 12, 1984, and will gradually become fully operative over the next 3 years. The act established an independent Data Protection Registrar with a staff of 20 to 30 members who are not civil servants. They are to maintain a register of personal data users and computer bureaus in the public and private sectors. Although the Home Office emphasizes that the law requires simple registration of automated systems rather than licensing, as in Sweden and France, the act requires quite complete information on each system and the users of the system. It remains to be seen whether there are any practical differences in terms of the amount of paperwork required.

Canada

Part IV of the Canadian Human Rights Act of 1977 introduced principles of fair information practice for the Federal public sector and created the position of Privacy Commissioner. The powers of the Commissioner consisted primarily in responding to complaints from individuals about denials of individual access to government personal data. The current Privacy Commissioner was a member of the Canadian Human Rights Commission.

In 1982, the Federal Privacy Act supplanted and significantly strengthened the privacy provisions of the Human Rights Act. Sections 4 to 10 of the 1982 act regulate the collection, retention, disposal, protection, and disclosure of personal information held by the Federal Government by means of a code of fair information practices. Its provisions are similar to the American Privacy Act. The Canadian law also specifies a list of 13 purposes for which a government institution may disclose personal information.

The Treasury Board is responsible for publishing an annual index of all the personal information systems maintained by the Federal Government in both manual and automated form, including the fewer than 25 systems that are exempt from access by individuals. The current edition runs to about 300 pages. Copies are available in post offices and libraries across Canada, but it is unusual to find persons who have consulted them.

The 1982 Privacy Act considerably strengthened the general powers of investigation and monitoring, and set up a separate Office of the Privacy Commissioner. The Privacy Commissioner holds office for 7 years, and is eligible for reappointment once. His independence is assured, in theory, by the fact that he is an officer of Parliament and is appointed by resolution of the Senate and House of Commons. In practice, the initial selection is in the hands of the government of the day; thereafter, the Privacy Commissioner has to retain the confidence of these two legislative bodies. Presently, the Information Commissioner, who is responsible for the law on access to government information, and the Privacy Commissioner share some administrative staff in the same office. The Privacy Commissioner has a legal advisor, a director of complaints and 5 investigators, and a director of compliance and 3 investigators, for a total of 15 direct staff and a share of 18 others.

The Privacy Commissioner has the overall responsibility to monitor the implementation of the Privacy Act. His recommendations to government departments are likely to carry a considerable amount of weight, although he does not have regulatory power, because he is an independent officer of Parliament. He can request a response from a department to one of his recommendations. He prepares an Annual Report to Parliament and may make special reports at his discretion. The act directs that a permanent committee of Parliament should review the administration of the statute. An individual may complain to the Privacy Commissioner about any alleged form of personal information misuse by the Federal Government. Moreover, the Commissioner has the power and resources to initiate and investigate a complaint himself.

Australia

In April 1976, the Australian Law Reform Commission was given a broad mandate to consider a variety of privacy issues, including data protection. After an exhaustive inquiry and the publication of a number of specialized reports, a comprehensive three-volume report was released at the end of 1983. With respect to its recommendations for data protection legislation, the Commission formulated 10 general principles for data protection modeled on the Organization for Economic Cooperation and Development's Guidelines. The Commission concluded that the private sector, as well as the public sector, should come within the ambit of legislation. It rejected the licensing model for data protection, but recommended the creation of a "statutory guardian" or "administrative body with the specific function of advocating privacy interests." Such a Privacy Commissioner would function primarily as an ombudsman, but would have regulatory power in one specific area—the handling of individual requests to obtain access to their own data and to amend incorrect records. In general, the basic functions of the Australian Privacy Commissioner would be similar to those of his or her counterpart in Canada and data protection officials in Western Europe.

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a non-voting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications; food and renewable resources; health; communication and information technologies; oceans and environment; and science, education, and transportation.

OTA-CIT-296

JUNE 1986